PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-099477
(43)Date of publication of application : 07.04.2000

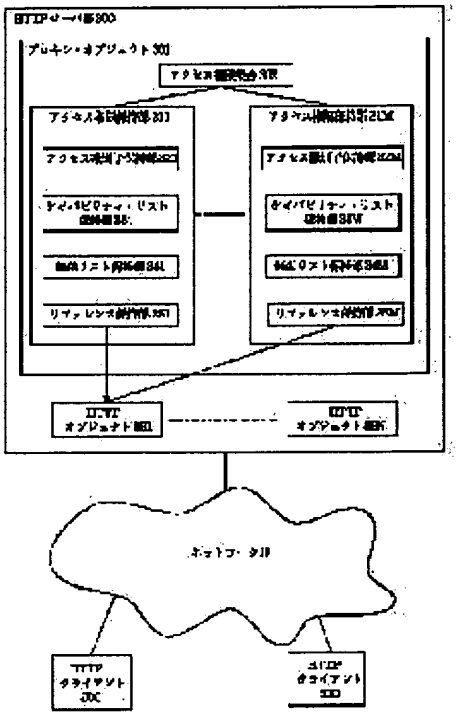
(51)Int.Cl. G06F 15/16
G06F 12/14
G06F 13/00

(21)Application number : 10-266141
(22)Date of filing : 21.09.1998

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : HORIKIRI KAZUNORI

(54) METHOD FOR MANAGING ACCESS TO OBJECT

(57)Abstract:
PROBLEM TO BE SOLVED: To safely protect objects existing on a network by providing the method with a step for connecting 1st authority information to an access identifier (ID) by an access management server and enciphering the connected information by applying a public key owned by the server itself to generate a 1st access key and other steps.
SOLUTION: A proxy object 301 generates an access ID and authority information for the ID. Then the object 301 connects the authority information to the access ID and enciphers the connected information by a public key to generate an access key. An HTTP client 50C receives the access key by message exchange using a cipher such as a secure socket layer(SSL) to/from an HTTP server 300. The client 50C receiving the access key connects authority information prepared by itself to a random number generated by itself and enciphers the connected information by the public key to generate an access key.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－99477
（P2000－99477A）
(43)公開日　平成12年４月７日(2000.4.7)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	15/16	６２０	Ｇ０６Ｆ 15/16	６２０Ｔ	
	12/14	３１０	12/14	３１０Ｋ	
	13/00	３５１	13/00	３５１Ｚ	

審査請求　未請求　請求項の数16　ＯＬ　（全 23 頁）

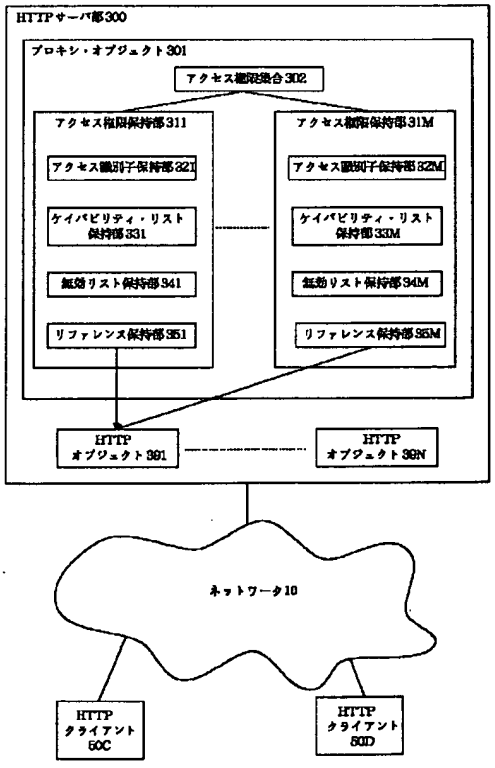
(21)出願番号　特願平10－266141

(22)出願日　平成10年９月21日(1998.9.21)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　堀切　和典
神奈川県足柄上郡中井町境430　グリーンテクなかい　富士ゼロックス株式会社内
(74)代理人　100086531
弁理士　澤田　俊夫

(54)【発明の名称】　オブジェクトのアクセス管理方法

(57)【要約】
【課題】　権限内容を変更したケイパビリティをクライアントが自由に生成し、他のクライアントに安全に委譲することができる、オブジェクトのアクセス管理方式を提供する。
【解決手段】　アクセス識別子やケイパビリティなどの秘密情報は、暗号鍵若しくは一方向性関数によって暗号化された形態でネットワーク上を伝送されるので、オブジェクトにアクセスするためのアクセス・キーが不正に使用される可能性は極めて低い。また、新たに生成した権限情報をアクセス・キーに連結して暗号化することによって新たなアクセス・キーを派生することを許容しているので、権限情報のバリエーションを増大させることができる。ケイパビリティの保持者には、さらに派生したアクセス・キーを無効化する権限も与えられる。



1

【特許請求の範囲】

【請求項１】オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトを要求する１以上のオブジェクト・クライアントと、あるオブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上におけるオブジェクトのアクセス管理方法であって、（ａ）アクセス管理サーバが、オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成するステップと、（ｂ）アクセス管理サーバが、第１の権限情報P_1とアクセス識別子ａとを連結し、自身が持つ公開鍵暗号系の公開鍵ｐｋｅｙを適用して暗号化し、第１のアクセス・キーａｋｅｙ$_1$＝ｐｋｅｙ（P_1，ａ）を生成するステップと、（ｃ）第１のアクセス・キーａｋｅｙ$_1$がオブジェクト・クライアントに配布されるステップと、（ｄ）第Ｎ－１のアクセス・キーａｋｅｙ$_{N-1}$を持つオブジェクト・クライアントが、第Ｎの権限情報P_Nを生成して、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キーａｋｅｙ$_{N-1}$とを連結して、公開鍵ｐｋｅｙを適用して暗号化し、第Ｎのアクセス・キーａｋｅｙ$_N$＝ｐｋｅｙ（P_N，ａｋｅｙ$_{N-1}$）を生成するステップと（但し、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｅ）オブジェクト・クライアントが、第Ｎのアクセス・キーａｋｅｙ$_N$を提示してオブジェクトＡへのアクセスを要求するステップと、（ｆ）アクセス管理サーバが、自身が持つ公開鍵暗号系の秘密鍵ｓｋｅｙを用いて第Ｎのアクセス・キーａｋｅｙ$_N$を復号化して、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キーａｋｅｙ$_{N-1}$を得て、これらを検査するステップと、（ｇ）アクセス管理サーバが、前記（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容するステップと、を含むことを特徴とするオブジェクトのアクセス管理方法。

【請求項２】オブジェクトを提供する１以上のオブジェクト・サーバとオブジェクトを要求する１以上のオブジェクト・クライアントとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを管理するためのアクセス管理サーバであって、（ａ）公開鍵暗号系の公開鍵ｐｋｅｙと秘密鍵ｓｋｅｙを保持する手段と、（ｂ）オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成する手段と、（ｃ）第１の権限情報P_1とアクセス識別子ａとを連結し、公開鍵ｐｋｅｙを適用して暗号化し、第１のアクセス・キーａｋｅｙ$_1$＝ｐｋｅｙ（P_1，ａ）を生成する手段と、（ｄ）第１のアクセス・キーａｋｅｙ$_1$をオブジェクト・クライアントに配布する手段と、（ｅ）第Ｎのアクセス・キーａｋｅｙ$_N$を提示したオブジェクトＡへのアクセス要求を受信する手段と（但し、第Ｎのアクセス・キーａｋｅｙ$_N$は、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キーａｋｅｙ$_{N-1}$を連結し、公開鍵ｐｋｅｙを適用して生成されたアクセス・キーｐｋｅｙ（P_N，ａｋｅｙ$_{N-1}$）のことであり、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｆ）秘密鍵ｓｋｅｙを用いて第Ｎのアクセス・キーａｋｅｙ$_N$を復号化して、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キーａｋｅｙ$_{N-1}$を得て、これらを検査する手段と、（ｇ）前記手段（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容する手段と、を含むことを特徴とするアクセス管理サーバ。

【請求項３】前記手段（ｆ）は、最初のアクセス識別子ａが現れるまで、秘密鍵ｓｋｅｙを用いた復号化処理を再帰的に実行することを特徴とする請求項２に記載のアクセス管理サーバ。

【請求項４】前記手段（ｆ）は、秘密鍵ｓｋｅｙを用いた復号化処理によって順次得られた各権限情報P_1，P_2，…，P_{N-1}，P_Nのコンテキストをも検査することを特徴とする請求項３に記載のアクセス管理サーバ。

【請求項５】さらに無効化されたアクセス・キーを保持する無効アクセス・キー・テーブルと、
オブジェクト・クライアントから無効化要求された第Ｍのアクセス・キーａｋｅｙＭを前記無効アクセス・キー・テーブルに登録する手段とを含み、
前記手段（ｆ）は、秘密鍵ｓｋｅｙを用いて第Ｎのアクセス・キーａｋｅｙ$_{N-1}$を再帰的に復号化処理する途中で無効化されたアクセス・キーａｋｅｙ$_N$を得ると、検査を失敗させ、オブジェクトＡへのアクセスを拒絶する、ことを特徴とする請求項３又は４のいずれかに記載のアクセス管理サーバ。

【請求項６】オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを要求するクライアントであって（但し、アクセス管理サーバは、公開鍵暗号系の公開鍵ｐｋｅｙと秘密鍵ｓｋｅｙを保持するものとする）、（ａ）アクセス識別子ａと第１の権限情報P_1を与えられたオブジェクトＡについての第Ｎ－１のアクセス・キーａｋｅｙ$_{N-1}$を受信する手段と、（ｂ）第Ｎの権限情報P_Nを生成する手段と、（ｃ）第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キーａｋｅｙ$_{N-1}$とを連結して、公開鍵ｐｋｅｙを適用して暗号化し、第Ｎのアクセス・キーａｋｅｙ$_N$＝ｐｋｅｙ（P_N，ａｋｅｙ$_{N-1}$）を生成する手段と、（ｄ）第Ｎのアクセス・キーａｋｅｙ$_N$を用いてオブジェクトＡへのアクセスを要求し、第Ｎのアクセス・キーａｋｅｙ$_N$を他のオブジェクト・クライアントに委譲し、又は、第Ｎのアクセス・キーａｋｅｙ$_N$の無効化を要求する手段と、を含むことを特徴とするオブジェク

ト・クライアント。

【請求項７】オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトを要求する１以上のオブジェクト・クライアントと、あるオブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上におけるオブジェクトのアクセス管理方法であって、（ａ）アクセス管理サーバが、オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成するステップと、（ｂ）アクセス管理サーバが、第１の権限情報P_1とアクセス識別子ａに対して一方向性関数ｆを適用して、第１のアクセス・キー$akey_1 = f(P_1, a)$を生成するステップと、（ｃ）第１のアクセス・キー$akey_1$がオブジェクト・クライアントに配布されるステップと、（ｄ）第Ｎ－１のアクセス・キー$akey_{N-1}$を持つオブジェクト・クライアントが、第Ｎの権限情報P_Nを生成し、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して一方向性関数ｆを適用して、第Ｎのアクセス・キー$akey_N = f(P_N, akey_{N-1})$を生成するステップと（但し、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｅ）オブジェクト・クライアントが、第Ｎのアクセス・キー$akey_N$と、各権限情報P_1，P_2，…，P_{N-1}，P_Nを提示して、オブジェクトＡへのアクセスを要求するステップと、（ｆ）アクセス管理サーバが、オブジェクトＡのアクセス識別子ａと受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nに対して一方向性関数ｆを順次適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査するステップと、（ｇ）アクセス管理サーバが、前記（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容するステップと、を含むことを特徴とするオブジェクトのアクセス管理方法。

【請求項８】オブジェクトを提供する１以上のオブジェクト・サーバとオブジェクトを要求する１以上のオブジェクト・クライアントとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを管理するためのアクセス管理サーバであって、（ａ）一方向性関数ｆを提供する手段と、（ｂ）オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成する手段と、（ｃ）第１の権限情報P_1とアクセス識別子ａに対して一方向性関数ｆを適用して、第１のアクセス・キー$akey_1 = f(P_1, a)$を生成する手段と、（ｄ）第１のアクセス・キー$akey_1$をオブジェクト・クライアントに配布する手段と、（ｅ）第Ｎのアクセス・キー$akey_N$と各権限情報P_1，P_2，…，P_{N-1}，P_Nを提示したオブジェクトＡへのアクセス要求を受信する手段と（但し、第Ｎのアクセス・キー$akey_N$は、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して一方向性関数ｆを適用して生成されたアクセス・キーｆ（P_N，$akey_{N-1}$）のことであり、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｆ）オブジェクトＡのアクセス識別子ａと受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nに対して一方向性関数ｆを順次適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査する手段と、（ｇ）前記手段（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容する手段と、を含むことを特徴とするアクセス管理サーバ。

【請求項９】前記手段（ｆ）は、受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nのコンテキストをも検査することを特徴とする請求項８に記載のアクセス管理サーバ。

【請求項１０】さらに無効化されたアクセス・キーを保持する無効アクセス・キー・テーブルと、

オブジェクト・クライアントから無効化要求された第Ｍのアクセス・キー$akey_M$を前記無効アクセス・キー・テーブルに登録する手段とを含み、

前記手段（ｆ）は、一方向性関数ｆを順次適用して第Ｎのアクセス・キー$akey_N$を生成する途中で無効化されたアクセス・キー$akey_M$を得ると、検査を失敗させ、オブジェクトＡへのアクセスを拒絶する、ことを特徴とする請求項９に記載のアクセス管理サーバ。

【請求項１１】オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを要求するクライアントであって（但し、アクセス管理サーバは、一方向性関数ｆを提供するものとする）、（ａ）アクセス識別子ａと第１の権限情報P_1を与えられたオブジェクトＡについての第Ｎ－１のアクセス・キー$akey_{N-1}$と各権限情報P_1，P_2，…，P_{N-1}を受信する手段と、（ｂ）第Ｎの権限情報P_Nを生成する手段と、（ｃ）第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して一方向性関数を適用して、第Ｎのアクセス・キー$akey_N = f(P_N, akey_{N-1})$を生成する手段と、（ｄ）第Ｎのアクセス・キー$akey_N$に各権限情報$P_1$，$P_2$，…，$P_{N-1}$を添えて、オブジェクトＡへのアクセスを要求し、第Ｎのアクセス・キー$akey_N$を他のオブジェクト・クライアントに委譲し、又は、第Ｎのアクセス・キー$akey_N$の無効化を要求する手段と、を含むことを特徴とするオブジェクト・クライアント。

【請求項１２】オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトを要求する１以上のオブジェクト・クライアントと、あるオブジェクトへのアクセスを管理するアクセス管理サーバとがネットワーク

を介して接続された分散型ネットワーク・システム上におけるオブジェクトのアクセス管理方法であって、
（ａ）アクセス管理サーバが、オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成するステップと、
（ｂ）アクセス管理サーバが、第１の権限情報P_1とアクセス識別子ａに対して可換な一方向性関数ｆを適用して、第１のアクセス・キー$akey_1 = f(P_1, a)$を生成するステップと、（ｃ）第１のアクセス・キー$akey_1$がオブジェクト・クライアントに配布されるステップと、（ｄ）第Ｎ－１のアクセス・キー$akey_{N-1}$を持つオブジェクト・クライアントが、第Ｎの権限情報P_Nを生成し、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して可換な一方向性関数ｆを適用して、第Ｎのアクセス・キー$akey_N = f(P_N, akey_{N-1})$を生成するステップと（但し、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｅ）オブジェクト・クライアントが、第Ｎのアクセス・キー$akey_N$と、各権限情報P_1，P_2，…，P_{N-1}，P_Nを提示して、オブジェクトＡへのアクセスを要求するステップと、（ｆ）アクセス管理サーバが、オブジェクトＡのアクセス識別子ａと受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nに対して可換な一方向性関数ｆを任意の順番で適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査するステップと、（ｇ）アクセス管理サーバが、前記（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容するステップと、を含むことを特徴とするオブジェクトのアクセス管理方法。
【請求項１３】オブジェクトを提供する１以上のオブジェクト・サーバとオブジェクトを要求する１以上のオブジェクト・クライアントとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを管理するためのアクセス管理サーバであって、（ａ）可換な一方向性関数ｆを提供する手段と、（ｂ）オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成する手段と、（ｃ）第１の権限情報P_1とアクセス識別子ａに対して可換な一方向性関数ｆを適用して、第１のアクセス・キー$akey_1 = f(P_1, a)$を生成する手段と、（ｄ）第１のアクセス・キー$akey_1$をオブジェクト・クライアントに配布する手段と、（ｅ）第Ｎのアクセス・キー$akey_N$と各権限情報P_1，P_2，…，P_{N-1}，P_Nを提示したオブジェクトＡへのアクセス要求を受信する手段と（但し、第Ｎのアクセス・キー$akey_N$は、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して可換な一方向性関数ｆを適用して生成されたアクセス・キー$f(P_N, akey_{N-1})$のことであり、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｆ）オブジェクトＡのアクセス識別子ａと受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nに対して可換な一方向性関数ｆを任意の順番で適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査する手段と、（ｇ）前記手段（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容する手段と、を含むことを特徴とするアクセス管理サーバ。
【請求項１４】前記手段（ｆ）は、受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nのコンテキストをも検査することを特徴とする請求項１３に記載のアクセス管理サーバ。
【請求項１５】さらに無効化されたアクセス・キーを保持する無効アクセス・キー・テーブルと、
オブジェクト・クライアントから無効化要求された第Ｍのアクセス・キー$akey_M$を前記無効アクセス・キー・テーブルに登録する手段とを含み、
前記手段（ｆ）は、可換な一方向性関数ｆを任意の順番で適用して第Ｎのアクセス・キー$akey_N$を生成する途中で無効化されたアクセス・キー$akey_M$を得ると、検査を失敗させ、オブジェクトＡへのアクセスを拒絶する、ことを特徴とする請求項１３に記載のアクセス管理サーバ。
【請求項１６】オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを要求するクライアントであって（但し、アクセス管理サーバは、可換な一方向性関数ｆを提供するものとする）、（ａ）アクセス識別子ａと第１の権限情報P_1を与えられたオブジェクトＡについての第Ｎ－１のアクセス・キー$akey_{N-1}$と各権限情報P_1，P_2，…，P_{N-1}を受信する手段と、（ｂ）第Ｎの権限情報P_Nを生成する手段と、（ｃ）第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して可換な一方向性関数を適用して、第Ｎのアクセス・キー$akey_N = f(P_N, akey_{N-1})$を生成する手段と、（ｄ）第Ｎのアクセス・キー$akey_N$に各権限情報$P_1$，$P_2$，…，$P_{N-1}$を添えて、オブジェクトＡへのアクセスを要求し、第Ｎのアクセス・キー$akey_N$を他のオブジェクト・クライアントに委譲し、又は、第Ｎのアクセス・キー$akey_N$の無効化を要求する手段と、を含むことを特徴とするオブジェクト・クライアント。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク上に複数のコンピュータ・システムが相互接続された分散型のネットワーク・システムにおいて、ネットワーク上に存在するオブジェクトを安全に保護するためのオブジェ

クトのアクセス管理方式に係り、特に、オブジェクトのアクセス権限を記述したケイパビリティ（Ｃａｐａｂｉｌｉｔｙ）をクライアントに配ることによってオブジェクトへのアクセスを許可するタイプのアクセス管理方式に関する。

【０００２】また、本発明は、ネットワーク・システム上のクライアント間でオブジェクトへのアクセス権限を与えることができるオブジェクトのアクセス管理方式に係り、特に、アクセス権限を記述したケイパビリティを安全に委譲したりケイパビリティを無効化することができるオブジェクトのアクセス管理方式に関する。

【０００３】

【従来の技術】昨今の情報処理・情報通信の分野における発展は目覚しいものがある。この種の技術分野においては、コンピュータ・システム同士を相互接続する、すなわち「コンピュータ・ネットワーキング」に関する研究・開発は、従来より活発に行われてきた。システム同士を相互接続する主な目的は、複数ユーザによるコンピュータ資源の共有や、情報の共有・流通などである。

【０００４】システム間を接続するための伝送媒体すなわち「ネットワーク」としては、大学や事業所の構内など限られた空間内に敷設されたＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）の他、ＬＡＮを専用回線で接続したＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）や、一般公衆回線（ＰＳＴＮ）、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ Ｓｅｒｖｉｃｅ Ｄｉｇｉｔａｌ Ｎｅｔｗｏｒｋ）、インターネットなど様々である。

【０００５】ネットワーク・システムは、一般に、ネットワーク上の特定のコンピュータをサーバ（ファイル・サーバ，プリント・サーバ）とし、これを他のクライアントが利用し合うというクライアント・サーバ・モデルとして構築される。また、ネットワーク上においては、各コンピュータ間でアプリケーションを分散処理する分散環境が実現されている。

【０００６】また、ネットワーク上には、無数のオブジェクトが存在する。例えばサーバはサービス・オブジェクトを所有し、これに対し、クライアントは、遠隔手続呼び出し（Ｒｅｍｏｔｅ Ｐｒｏｃｅｄｕｒｅ Ｃａｌｌ：ＲＰＣ）、又は、遠隔メソッド呼び出し（Ｒｅｍｏｔｅ Ｍｅｔｈｏｄ Ｉｎｖｏｃａｔｉｏｎ：ＲＭＩ）などを用いて遠隔的にサービスを要求することができる。ネットワークがＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）接続で構成されるインターネットであり、サーバがＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）サーバであれば、ＨＴＴＰサーバが所有するサービス・オブジェクトの実体は、ＨＴＴＰクライアントにおいてホームページを形成するためのＨＴＭＬ（Ｈｙｐｅｒ Ｔｅｘｔ Ｍａｒｋｕｐ Ｌａｎｇｕａｇｅ）ファイルである。ＨＴＴＰクライアントは、例えばＵＲＬ（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ）によってサービス要求を行うことができる。

【０００７】ところで、オブジェクトに対するアクセスは、一般には、オブジェクト自身が持つアクセス識別子を参照することによって実現される。アクセス識別子は、例えばオブジェクトの名前（オブジェクト識別子）であることもある。例えば、オブジェクトの実体がファイルであれば、識別子としてのファイル名をファイル・システムに提示することによりファイル・アクセスを果たすことができる。また、ＨＴＴＰサーバ・クライアントで構成されるＷＷＷ空間では、ＵＲＬがオブジェクトの識別子に相当する。アクセス識別子は、１つのオブジェクトに対して一対一だけではなく、１つのオブジェクトが複数のアクセス識別子を用意することもある。

【０００８】他方、最近では、オブジェクトへのアクセスを制限という技術に関して研究開発が進められている。特に、ネットワーク上にオブジェクトが散在し、複数のクライアントがアクセスを試みるような分散ネットワーク環境においては、セキュリティの観点からもアクセス制御は非常に重要な課題である。

【０００９】オブジェクトに対するアクセスを制限するための方式の１つとして、「ケイパビリティ（Ｃａｐａｂｉｌｉｔｙ）」方式がある。ケイパビリティとは、オブジェクトに対するアクセス権限のことである。例えば、アクセスが許可されている有効期限や、許可された残りアクセス回数、許可された操作（読み出し、書き込み、実行など）などがケイパビリティに含まれる項目である。ケイパビリティ方式によれば、オブジェクトは、自身に用意された複数のアクセス識別子の各々に対して異なったケイパビリティを与えることもできる。例えば、あるアクセス識別子ａ１に対しては有効アクセス回数を１０回に設定する一方、他のアクセス識別子ａ２には３回のアクセスに制限したりする。あるいは、アクセス識別子ａ１には読み出し、書きこみ、実行、削除など全ての操作権限を与えるが、アクセス識別子ａ２には読出ししか許さないようにすることもできる。

【００１０】ケイパビリティは、オブジェクトへのアクセスを許容する一種の鍵の役割を持つ。すなわち、ケイパビリティを所有するクライアントは、オブジェクトへのアクセスを許可される。例えば、ネットワークが無数のコンピュータ・システムがＴＣＰ／ＩＰ接続されてなるインターネットのような場合には、ケイパビリティをＵＲＬ文字列の中で記述することもできる。

【００１１】ところで、クライアント・ユーザは、ネットワーク上に散在する有益なリソースすなわちオブジェクトを、他のユーザと共有することを望むことがある。例えば、クライアントＡ（上司）が、自分の不在中に、クライアントＢ（部下）にオブジェクトの管理を委ねたいような場合である。この場合、クライアントＡは、他

のクライアントＢに対してケイパビリティを委譲することによって、ある１つのオブジェクトを共有することができる。

【００１２】ところが、クライアントが、自分と同じケイパビリティを他人に与えてしまっては、オブジェクトが思わぬ不利益を被ることがある。上記の例で言えば、クライアントＡが、クライアントＢに自分と同じケイパビリティを委譲してしまうと、クライアントＡが職場に復帰した後もクライアントＢはオブジェクトにアクセスし続けることができる。また、クライアントＢはオブジェクトの読み出しオペレーションだけを許可すれば充分なのに、クライアントＡと等しく書き込みや実行オペレーションまで不用意に許可してしまっては、オブジェクトに対して不測の改竄が加えられかねない。

【００１３】要言すれば、ネットワーク・システムの運用上、ケイパビリティの委譲を認めるべきではある一方、ケイパビリティの委譲を無制限に許すとネットワークやオブジェクトのセキュリティは脅かされかねないのである。委譲の際には、操作権限に所定の制限を加えるなどなど、ケイパビリティを弱める必要がある。

【００１４】また、ケイパビリティを不正に改竄されないためにも、ケイパビリティの譲受者に対しては、ケイパビリティの内容すら秘匿すべきである。ネットワーク上では、オブジェクトに対するアクセス識別子やそのケイパビリティは、そもそも、秘密情報としての性格が強い。

【００１５】更に言えば、オブジェクトへのアクセスを管理するサーバは、クライアントが生成したケイパビリティを安全且つ確実に検査する必要がある。

【００１６】また、ケイパビリティを生成したクライアントは、オブジェクトが危険にさらされるなどの所定の事態の検知若しくは予見によって、生成したケイパビリティを無効化する必要もあるであろう。

【００１７】例えば特開平５－８１２０４号公報には、分散型コンピュータ・システムにおけるアクセス制御について開示されている。同公報によれば、ケイパビリティに相当する特権属性証明書（ＰＡＣ）の代理使用を制御すると同時に、ＰＡＣを多くの目的のために使用できる方法が提供されている。すなわち、ＰＡＣを配布する際には、これに開始者実体に相当する開始者資格付与属性を含めるようにするとともに、暗号的に開始者資格付与属性を有した暗号キーを開始者実体に配布するようになっている。

【００１８】しかしながら、特開平５－８１２０４号公報に開示された方法によれば、使用期限やアクセス回数など、ケイパビリティーのバリエーションには対応できない。また、開始実体者がケイパビリティを弱めたＰＡＣを自由に作成する方法については一切言及していない。

【００１９】また、特開平９－３１９６５９号公報には、非分散型のコンピュータ・システムにおいて、各ユーザに異なるケイパビリティを割り当てる方式について開示されている。同公報によれば、コンピュータ機能の全体はケイパビリティ・セットを有するイベント・セットに細分化されており、ユーザがコンピュータ・システム上で実行しようとする特定のジョブに応じてケイパビリティが与えられるようになっている。しかしながら、特開平９－３１９６５９号公報に係る発明は、ケイパビリティを安全に守ることができない分散環境に適用されたものではない。また、同公報は、オブジェクト間でケイパビリティの検査を安全に行う方法については一切言及していない。

【００２０】また、特開平９－２５１４２５号公報には、分散システムにおけるシステム資源へのアクセスのセキュリティ制御について開示している。すなわち、グループ識別標識を記憶しておき、これをターゲット・オブジェクトに結び付け、次にメンバーシップ検査を使用して、ターゲット・オブジェクトへのアクセスを要求するクライアントがターゲットに対するアクセス権限を有するグループ・メンバーであるか否かを判断するようになっている。

【００２１】しかしながら、特開平９－２５１４２５号公報では、使用期限やアクセス回数など、ケイパビリティーのバリエーションには対応する手法については開示していない。また、あるケイパビリティの保有者が新たにケイパビリティを生成したりこれを無効化する手法についても一切言及していない。

【００２２】また、分散ＯＳ（オペレーティング・システム）として当業界では周知の”Ａｍｏｅｂａ”は、譲渡可能で且つ偽造が困難なケイパビリティを提供している。これは以下の機構により実現される。

（１）クライアントがオブジェクト生成要求をサーバに送信する。

（２）サーバは、オブジェクトを生成して、オブジェクト番号と乱数を割り当てる。乱数は、オブジェクト番号でインデックス付けされたオブジェクト・テーブルに格納される。

（３）サーバは、乱数をキーとして権限と乱数を暗号化したチェック・フィールドを含むケイパビリティを生成する。

（４）ケイパビリティをクライアントに返す。

（５）クライアントが、サーバに対して、ケイパビリティを提示したアクセス要求を出す。

（６）サーバは、ケイパビリティからオブジェクト番号とチェック・フィールドを抽出し、オブジェクト・テーブルに格納されている乱数を基にチェック・フィールドから権限と乱数を復号化する。

（７）復号の結果得られた乱数がオブジェクト・テーブルに格納された乱数と一致するかどうか検証する。

（８）要求された操作がケイパビリティに記述された権

限に合致すれば、サーバはその操作を実行する。

【００２３】Ａｍｏｅｂａでは、さらに、ケイパビリティの保持者が権限を弱めた新しいケイパビリティを生成するために、以下の機構も備えている。

（１）クライアントとサーバがＮ個の可換な一方向性関数を共有する。

（２）クライアントが第２の権限を生成する。

（３）　クライアントが第１の権限と第２の権限との差分の権限に該当する番号と対応付けた一方向性関数を全て適用して、第２のチェック・フィールドを生成する。

（４）サーバが、第２の権限と第２のチェック・フィールドを含むケイパビリティを受信する。

（５）サーバは、権限フィールドに従い、一方向性関数を順次適用して、クライアントが提示したチェック・フィールドと一致した場合に、その操作を実行する。

【００２４】しかしながら、Ａｍｏｅｂａは、Ｎ個の可換な一方向性関数を用いてＮ個の権限の可否を記述する方法については規定しているが、使用権限や回数といった権限についての多くのバリエーションに対応する点については考慮していない。また、ケイパビリティーの無効化に関しては、サーバで保持されている乱数を変更することによってあるオブジェクトについての全てのケイパビリティを無効化する手法が規定されているが、特定のケイパビリティを無効化する手法については言及していない。例えば、あるケイパビリティの保持者が生成したケイパビリティや、これから派生したケイパビリティのみを無効化する点は一切規定していない。

【００２５】また、Ａｍｏｅｂａではオブジェクトにアクセスするためのオブジェクト番号自体については一切プロテクトがかけられていない。

【００２６】また、Ｗｅｂ上で公開されたＢｊｏｒｎ Ｎ．Ｆｒｅｅｍａｎ－Ｂｅｎｓｏｎの論文”Ｕｓｉｎｇ ｔｈｅ Ｗｅｂ ｔｏ Ｐｒｉｖａｔｅ Ｉｎｆｏｒｍａｔｉｏｎ －ｏｒ－ Ａ Ｓｈｏｒｔ Ｐａｐｅｒ Ａｂｏｕｔ Ｐａｓｓｗｏｒｄ Ｐｒｏｔｅｃｔｉｏｎ Ｗｉｔｈｏｕｔ Ｃｌｉｅｎｔ Ｍｏｄｉｆｉｃａｔｉｏｎ”（ＵＲＬは”ｈｔｔｐ：／／ｗｗｗｌ．ｃｅｒｎ．ｃｈ／ｗｗｗ９４／ＰｒｅｌｉｍＰｒｏｃｓ．ｈｔｍｌ”）では、機密性のあるＵＲＬ（すなわちケイパビリティ）の取り扱いについて開示されている。同論文に記載された方式は以下の手順に従う。

（１）サーバがログイン名とパスワードの組からなるパスワード・リストを生成・保持する。また、サーバは暗号鍵を保持している。

（２）クライアントがログイン名とパスワードの組からなるメッセージをサーバに送信する。

（３）サーバは、パスワード・リストを検索し、クライアントから送信されたログイン名とパスワードの組が見つかれば、このログイン名とパスワードを暗号鍵で暗号化した文字列をアクセス・キーとして、ＵＲＬに含めてクライアントに送信する。

（４）クライアントは、受け取ったＵＲＬを用いてサーバにアクセス要求する。

（５）サーバは、受信したＵＲＬからアクセス・キーを抽出し、暗号鍵を用いて復号化して、もとのログイン名とパスワードの組を得る。そして、これがパスワード・リストに登録されているかどうかを検査する。

（６）登録されていれば、サーバは対応するオブジェクトへのアクセスを許可する。

【００２７】また、同論文では、クライアントがパスワードの変更を行うことでＵＲＬを無効化することができる点を言及している。

【００２８】しかしながら、同論文では、ある１つのオブジェクトについての正当で且つ異なるＵＲＬ（すなわちケイパビリティ）を複数生成する点については開示していない。また、パスワードの保持者ではなくＵＲＬ（すなわちケイパビリティ）の保持者がＵＲＬを無効化する点についても一切言及していない。

【００２９】

【発明が解決しようとする課題】本発明の目的は、ネットワーク上に複数のコンピュータ・システムが相互接続された分散型のネットワーク・システムにおいて、ネットワーク上に存在するオブジェクトを安全に保護することができる、優れたオブジェクトのアクセス管理方式を提供することにある。

【００３０】本発明の更なる目的は、オブジェクトのアクセス権限を記述したケイパビリティ（Ｃａｐａｂｉｌｉｔｙ）をクライアントに配ることによってオブジェクトへのアクセスを許可するタイプの、優れたアクセス管理方式を提供することにある。

【００３１】本発明の更なる目的は、ケイパビリティを保有するクライアントが権限を変更したケイパビリティを自由に生成し、他のクライアントに安全に委譲することができる、優れたオブジェクトのアクセス管理方式を提供することにある。

【００３２】本発明の更なる目的は、ケイパビリティを保有するクライアントが権限を変更したケイパビリティを自由に生成し、オブジェクトを管理するサーバは生成されたケイパビリティを安全に検査することができる、優れたオブジェクトのアクセス管理方式を提供することにある。

【００３３】本発明の更なる目的は、ケイパビリティを保有するクライアントが権限を変更したケイパビリティを自由に生成し、さらに生成したケイパビリティを確実に無効化することができる、オブジェクトのアクセス管理方式を提供することにある。

【００３４】

【課題を解決するための手段】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、オブジェクトを提供する１以上のオブジェクト・サーバと、オ

ブジェクトを要求する１以上のオブジェクト・クライアントと、あるオブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上におけるオブジェクトのアクセス管理方法であって、（ａ）アクセス管理サーバが、オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成するステップと、（ｂ）アクセス管理サーバが、第１の権限情報P_1とアクセス識別子ａとを連結し、自身が持つ公開鍵暗号系の公開鍵ｐｋｅｙを適用して暗号化し、第１のアクセス・キー$akey_1$＝ｐｋｅｙ（P_1，ａ）を生成するステップと、（ｃ）第１のアクセス・キー$akey_1$がオブジェクト・クライアントに配布されるステップと、（ｄ）第Ｎ－１のアクセス・キー$akey_{N-1}$を持つオブジェクト・クライアントが、第Ｎの権限情報P_Nを生成して、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$とを連結して、公開鍵ｐｋｅｙを適用して暗号化し、第Ｎのアクセス・キー$akey_N$＝ｐｋｅｙ（P_N，$akey_{N-1}$）を生成するステップと（但し、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｅ）オブジェクト・クライアントが、第Ｎのアクセス・キー$akey_N$を提示してオブジェクトＡへのアクセスを要求するステップと、（ｆ）アクセス管理サーバが、自身が持つ公開鍵暗号系の秘密鍵ｓｋｅｙを用いて第Ｎのアクセス・キー$akey_N$を復号化して、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$を得て、これらを検査するステップと、（ｇ）アクセス管理サーバが、前記（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容するステップと、を含むことを特徴とするオブジェクトのアクセス管理方法である。

【００３５】また、本発明の第２の側面は、オブジェクトを提供する１以上のオブジェクト・サーバとオブジェクトを要求する１以上のオブジェクト・クライアントとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを管理するためのアクセス管理サーバであって、（ａ）公開鍵暗号系の公開鍵ｐｋｅｙと秘密鍵ｓｋｅｙを保持する手段と、（ｂ）オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成する手段と、（ｃ）第１の権限情報P_1とアクセス識別子ａとを連結し、公開鍵ｐｋｅｙを適用して暗号化し、第１のアクセス・キー$akey_1$＝ｐｋｅｙ（P_1，ａ）を生成する手段と、（ｄ）第１のアクセス・キー$akey_1$をオブジェクト・クライアントに配布する手段と、（ｅ）第Ｎのアクセス・キー$akey_N$を提示したオブジェクトＡへのアクセス要求を受信する手段と（但し、第Ｎのアクセス・キー$akey_N$は、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$を連結し、公開鍵ｐｋｅｙを適用して生成されたアクセス・キーｐｋｅｙ（P_N，$akey_{N-1}$）のことであり、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｆ）秘密鍵ｓｋｅｙを用いて第Ｎのアクセス・キー$akey_N$を復号化して、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$を得て、これらを検査する手段と、（ｇ）前記手段（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容する手段と、を含むことを特徴とするアクセス管理サーバである。

【００３６】ここで、前記手段（ｆ）は、最初のアクセス識別子ａが現れるまで、秘密鍵ｓｋｅｙを用いた復号化処理を再帰的に実行するようにしてもよい。

【００３７】また、前記手段（ｆ）は、秘密鍵ｓｋｅｙを用いた復号化処理によって順次得られた各権限情報P_1，P_2，…，P_{N-1}，P_Nのコンテキストをも検査するようにしてもよい。

【００３８】また、アクセス管理サーバは、さらに無効化されたアクセス・キーを保持する無効アクセス・キー・テーブルと、オブジェクト・クライアントから無効化要求された第Ｍのアクセス・キー$akey_M$を前記無効アクセス・キー・テーブルに登録する手段とを含み、前記手段（ｆ）は、秘密鍵ｓｋｅｙを用いて第Ｎのアクセス・キー$akey_{N-1}$を再帰的に復号化処理する途中で無効化されたアクセス・キー$akey_M$を得ると、検査を失敗させ、オブジェクトＡへのアクセスを拒絶するようにしてもよい。

【００３９】また、本発明の第３の側面は、オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを要求するクライアントであって（但し、アクセス管理サーバは、公開鍵暗号系の公開鍵ｐｋｅｙと秘密鍵ｓｋｅｙを保持するものとする）、（ａ）アクセス識別子ａと第１の権限情報P_1を与えられたオブジェクトＡについての第Ｎ－１のアクセス・キー$akey_{N-1}$を受信する手段と、（ｂ）第Ｎの権限情報P_Nを生成する手段と、（ｃ）第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$とを連結して、公開鍵ｐｋｅｙを適用して暗号化し、第Ｎのアクセス・キー$akey_N$＝ｐｋｅｙ（P_N，$akey_{N-1}$）を生成する手段と、（ｄ）第Ｎのアクセス・キー$akey_N$を用いてオブジェクトＡへのアクセスを要求し、第Ｎのアクセス・キー$akey_N$を他のオブジェクト・クライアントに委譲し、又は、第Ｎのアクセス・キー$akey_N$の無効化を要求する手段と、を含むことを特徴とするオブジェクト・クライアントである。

【００４０】また、本発明の第４の面は、オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェ

クトを要求する１以上のオブジェクト・クライアントと、あるオブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上におけるオブジェクトのアクセス管理方法であって、（ａ）アクセス管理サーバが、オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成するステップと、（ｂ）アクセス管理サーバが、第１の権限情報P_1とアクセス識別子ａに対して一方向性関数ｆを適用して、第１のアクセス・キー$akey_1 = f(P_1, a)$を生成するステップと、（ｃ）第１のアクセス・キー$akey_1$がオブジェクト・クライアントに配布されるステップと、（ｄ）第Ｎ－１のアクセス・キー$akey_{N-1}$を持つオブジェクト・クライアントが、第Ｎの権限情報P_Nを生成し、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して一方向性関数ｆを適用して、第Ｎのアクセス・キー$akey_N = f(P_N, akey_{N-1})$を生成するステップと（但し、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｅ）オブジェクト・クライアントが、第Ｎのアクセス・キー$akey_N$と、各権限情報$P_1, P_2, \cdots, P_{N-1}, P_N$を提示して、オブジェクトＡへのアクセスを要求するステップと、（ｆ）アクセス管理サーバが、オブジェクトＡのアクセス識別子ａと受信した各権限情報$P_1, P_2, \cdots, P_{N-1}, P_N$に対して一方向性関数ｆを順次適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査するステップと、（ｇ）アクセス管理サーバが、前記（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容するステップと、を含むことを特徴とするオブジェクトのアクセス管理方法である。

【００４１】また、本発明の第５の側面は、オブジェクトを提供する１以上のオブジェクト・サーバとオブジェクトを要求する１以上のオブジェクト・クライアントとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを管理するためのアクセス管理サーバであって、（ａ）一方向性関数ｆを提供する手段と、（ｂ）オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成する手段と、（ｃ）第１の権限情報P_1とアクセス識別子ａに対して一方向性関数ｆを適用して、第１のアクセス・キー$akey_1 = f(P_1, a)$を生成する手段と、（ｄ）第１のアクセス・キー$akey_1$をオブジェクト・クライアントに配布する手段と、（ｅ）第Ｎのアクセス・キー$akey_N$と各権限情報$P_1, P_2, \cdots, P_{N-1}, P_N$を提示したオブジェクトＡへのアクセス要求を受信する手段と（但し、第Ｎのアクセス・キー$akey_N$は、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して一方向性関数ｆを適用して生成されたアクセス・キーｆ（$P_N, akey_{N-1}$）のことであり、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｆ）オブジェクトＡのアクセス識別子ａと受信した各権限情報$P_1, P_2, \cdots, P_{N-1}, P_N$に対して一方向性関数ｆを順次適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査する手段と、（ｇ）前記手段（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容する手段と、を含むことを特徴とするアクセス管理サーバである。

【００４２】ここで、前記手段（ｆ）は、受信した各権限情報$P_1, P_2, \cdots, P_{N-1}, P_N$のコンテキストをも検査するようにしてもよい。

【００４３】また、アクセス管理サーバは、さらに無効化されたアクセス・キーを保持する無効アクセス・キー・テーブルと、オブジェクト・クライアントから無効化要求された第Ｍのアクセス・キー$akey_M$を前記無効アクセス・キー・テーブルに登録する手段とを含み、前記手段（ｆ）は、一方向性関数ｆを順次適用して第Ｎのアクセス・キー$akey_N$を生成する途中で無効化されたアクセス・キー$akey_M$を得ると、検査を失敗させ、オブジェクトＡへのアクセスを拒絶するようにしてもよい。

【００４４】また、本発明の第６の側面は、オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを要求するクライアントであって（但し、アクセス管理サーバは、一方向性関数ｆを提供するものとする）、（ａ）アクセス識別子ａと第１の権限情報P_1を与えられたオブジェクトＡについての第Ｎ－１のアクセス・キー$akey_{N-1}$と各権限情報$P_1, P_2, \cdots, P_{N-1}$を受信する手段と、（ｂ）第Ｎの権限情報$P_N$を生成する手段と、（ｃ）第Ｎの権限情報$P_N$と第Ｎ－１のアクセス・キー$akey_{N-1}$に対して一方向性関数を適用して、第Ｎのアクセス・キー$akey_N = f(P_N, akey_{N-1})$を生成する手段と、（ｄ）第Ｎのアクセス・キー$akey_N$に各権限情報$P_1, P_2, \cdots, P_{N-1}$を添えて、オブジェクトＡへのアクセスを要求し、第Ｎのアクセス・キー$akey_N$を他のオブジェクト・クライアントに委譲し、又は、第Ｎのアクセス・キー$akey_N$の無効化を要求する手段と、を含むことを特徴とするオブジェクト・クライアントである。

【００４５】また、本発明の第７の側面は、オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトを要求する１以上のオブジェクト・クライアントと、あるオブジェクトへのアクセスを管理するアクセス

管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上におけるオブジェクトのアクセス管理方法であって、（ａ）アクセス管理サーバが、オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成するステップと、（ｂ）アクセス管理サーバが、第１の権限情報P_1とアクセス識別子ａに対して可換な一方向性関数ｆを適用して、第１のアクセス・キー$akey_1=f(P_1, a)$を生成するステップと、（ｃ）第１のアクセス・キー$akey_1$がオブジェクト・クライアントに配布されるステップと、（ｄ）第Ｎ－１のアクセス・キー$akey_{N-1}$を持つオブジェクト・クライアントが、第Ｎの権限情報P_Nを生成し、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して可換な一方向性関数ｆを適用して、第Ｎのアクセス・キー$akey_N=f(P_N, akey_{N-1})$を生成するステップと（但し、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｅ）オブジェクト・クライアントが、第Ｎのアクセス・キー$akey_N$と、各権限情報P_1，P_2，…，P_{N-1}，P_Nを提示して、オブジェクトＡへのアクセスを要求するステップと、（ｆ）アクセス管理サーバが、オブジェクトＡのアクセス識別子ａと受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nに対して可換な一方向性関数ｆを任意の順番で適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査するステップと、（ｇ）アクセス管理サーバが、前記（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容するステップと、を含むことを特徴とするオブジェクトのアクセス管理方法である。

【００４６】また、本発明の第８の側面は、オブジェクトを提供する１以上のオブジェクト・サーバとオブジェクトを要求する１以上のオブジェクト・クライアントとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを管理するためのアクセス管理サーバであって、（ａ）可換な一方向性関数ｆを提供する手段と、（ｂ）オブジェクトＡにアクセスするためのアクセス識別子ａと、アクセス識別子ａに対する第１の権限情報P_1を生成する手段と、（ｃ）第１の権限情報P_1とアクセス識別子ａに対して可換な一方向性関数ｆを適用して、第１のアクセス・キー$akey_1=f(P_1, a)$を生成する手段と、（ｄ）第１のアクセス・キー$akey_1$をオブジェクト・クライアントに配布する手段と、（ｅ）第Ｎのアクセス・キー$akey_N$と各権限情報P_1，P_2，…，P_{N-1}，P_Nを提示したオブジェクトＡへのアクセス要求を受信する手段と（但し、第Ｎのアクセス・キー$akey_N$は、第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して可換な一方向性関数ｆを適用して生成されたアクセス・キーｆ（P_N，$akey_{N-1}$）のことであり、Ｎは正の整数であり、第０のアクセス・キーはアクセス識別子ａとする。）、（ｆ）オブジェクトＡのアクセス識別子ａと受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nに対して可換な一方向性関数ｆを任意の順番で適用して、改めて第Ｎのアクセス・キー$akey_N$を生成し、これと受信した第Ｎのアクセス・キー$akey_N$とを比較して検査する手段と、（ｇ）前記手段（ｆ）における検査が成功したことに応答して、オブジェクトＡへのアクセスを許容する手段と、を含むことを特徴とするアクセス管理サーバである。

【００４７】ここで、前記手段（ｆ）は、受信した各権限情報P_1，P_2，…，P_{N-1}，P_Nのコンテキストをも検査するようしてもよい。

【００４８】また、アクセス管理サーバは、さらに無効化されたアクセス・キーを保持する無効アクセス・キー・テーブルと、オブジェクト・クライアントから無効化要求された第Ｍのアクセス・キー$akey_M$を前記無効アクセス・キー・テーブルに登録する手段とを含み、前記手段（ｆ）は、可換な一方向性関数ｆを任意の順番で適用して第Ｎのアクセス・キー$akey_N$を生成する途中で無効化されたアクセス・キー$akey_M$を得ると、検査を失敗させ、オブジェクトＡへのアクセスを拒絶するようにしてもよい。

【００４９】また、本発明の第９の側面は、オブジェクトを提供する１以上のオブジェクト・サーバと、オブジェクトへのアクセスを管理するアクセス管理サーバとがネットワークを介して接続された分散型ネットワーク・システム上において、オブジェクトへのアクセスを要求するクライアントであって（但し、アクセス管理サーバは、可換な一方向性関数ｆを提供するものとする）、（ａ）アクセス識別子ａと第１の権限情報P_1を与えられたオブジェクトＡについての第Ｎ－１のアクセス・キー$akey_{N-1}$と各権限情報P_1，P_2，…，P_{N-1}を受信する手段と、（ｂ）第Ｎの権限情報P_Nを生成する手段と、（ｃ）第Ｎの権限情報P_Nと第Ｎ－１のアクセス・キー$akey_{N-1}$に対して可換な一方向性関数を適用して、第Ｎのアクセス・キー$akey_N=f(P_N, akey_{N-1})$を生成する手段と、（ｄ）第Ｎのアクセス・キー$akey_N$に各権限情報$P_1$，$P_2$，…，$P_{N-1}$を添えて、オブジェクトＡへのアクセスを要求し、第Ｎのアクセス・キー$akey_N$を他のオブジェクト・クライアントに委譲し、又は、第Ｎのアクセス・キー$akey_N$の無効化を要求する手段と、を含むことを特徴とするオブジェクト・クライアントである。

【００５０】

【作用】本発明に係るオブジェクトのアクセス管理方式によれば、アクセス識別子やケイパビリティなどの秘密情報は、暗号鍵若しくは一方向性関数によって暗号化された形態でネットワーク上を伝送される。したがって、

オブジェクトにアクセスするためのアクセス・キーが解読され、不正に使用される可能性は極めて低い。

【００５１】また、新たに生成した権限情報をアクセス・キーに連結して暗号化することによって新たなアクセス・キーを派生することを許容しているので、権限情報のバリエーションを増大させることができる。

【００５２】また、権限情報を生成したケイパビリティの保持者が、さらにケイパビリティを弱めた権限情報を連結して新たなアクセス・キーを生成することができるので、アクセス権限の委譲を安全に行うことができる。ケイパビリティの保持者には、さらに派生したアクセス・キーを無効化する権限も与えられる。

【００５３】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００５４】

【発明の実施の形態】１．第１の実施形態

本発明は、オブジェクトに対するアクセスを制御するためのものである。特に、複数のコンピュータ・システムがネットワークを介して接続されたネットワーク・システム上において、ネットワーク上に存在するオブジェクトに対するアクセスを制御するためのものである。

【００５５】ここで言うネットワークは、主として、各コンピュータ・システムでアプリケーションを分散処理する分散型ネットワークである。また、ネットワークに接続された各コンピュータ・システムは、オブジェクトを所有するオブジェクト・サーバ（以下、単に「サーバ」とする）と、オブジェクトへのアクセスを要求するオブジェクト・クライアント（以下、単に「クライアント」とする）とに２分される。

【００５６】ネットワーク上には、さらにオブジェクトへのアクセス管理（すなわちオブジェクトのセキュリティ管理）を行うためのアクセス管理サーバも存在する。アクセス管理サーバは、オブジェクト・サーバ自身がその機能を兼ね備えることができるし、あるいはネットワーク上の別のコンピュータ・システムにアクセス管理を委ねることもできる。

【００５７】アクセス管理サーバは、オブジェクトへのアクセスを管理するために、オブジェクトに対して１以上のアクセス識別子を生成する。アクセス識別子を提示することによってオブジェクトへのアクセスが許可される。

【００５８】アクセス識別子は、通常、所定の規則性に従って生成される。例えば識別子中に通し番号が含まれていれば、他のアクセス識別子を容易に推測することができ、オブジェクトのセキュリティが危うくなる。このため、アクセス管理サーバは、アクセス識別子そのものをクライアントに配布することはせずに、元のアクセス識別子に何らかの加工（例えば暗号化）を施したアクセス・キーを代わりに配布するようにしている。アクセス識別子ではなくアクセス・キーを提示することによっても、オブジェクトへのアクセスが許可される。

【００５９】また、セキュリティの観点からオブジェクトへのアクセス権限を制限する必要もある。アクセス権限とは、例えば許可されたアクセス回数（残りアクセス回数）や、アクセスの有効期限、許可されたオブジェクトへの操作（読み出し、書きこみ、削除、実行など）などである。当業界では、アクセスに関する権限情報のことを「ケイパビリティ（Ｃａｐａｂｉｌｉｔｙ）」とも呼ぶ。

【００６０】アクセス管理サーバは、アクセス識別子を生成するときには、そのアクセス識別子に与えられたケイパビリティも定義する。また、１つのオブジェクトに対して複数のアクセス識別子を生成することもできる。アクセス管理サーバは、各アクセス識別子とそのケイパビリティを、対応するオブジェクトと関連付けて保管するようになっている。また、アクセス識別子から派生したアクセス・キーを保管してもよい。また、アクセス管理サーバは、公開鍵暗号系の公開鍵ｐｋｅｙと秘密鍵ｓｋｅｙを有している。

【００６１】１．１　アクセス管理サーバでの操作

アクセス管理サーバは、まず、あるオブジェクトＡへのアクセスを許可するためのアクセス識別子ａを生成する。

【００６２】また、アクセス管理サーバは、アクセス識別子ａに対して第１の権限情報P_1を生成する。アクセス管理サーバは、アクセス識別子ａを第１の権限情報P_1と関連付けて保管する。

【００６３】次いで、アクセス管理サーバは、アクセス識別子ａと第１の権限情報P_1を連結（例えばビット連結）し、公開鍵ｐｋｅｙを適用することで暗号化して、第１のアクセス・キーｐｋｅｙ（P_1，ａ）を生成する。また、アクセス・管理サーバは、アクセス・キーｐｋｅｙ（P_1，ａ）を、オブジェクトＡと対応付けて保管しておく。第１の権限情報P_1は、公開鍵ｐｋｅｙで暗号化されているので、アクセス管理サーバ以外は解読することができない。

【００６４】１．２　クライアントでの操作

生成された第１のアクセス・$akey_1$＝ｐｋｅｙ（P_1，ａ）は、例えばネットワーク経由で、あるクライアントに委譲されたとする。第１のアクセス・キーはアクセス管理サーバの公開鍵ｐｋｅｙで暗号化されているので、これを使用するクライアントは原則として、自身に与えられた権限情報Ｐ１の内容を判読できない。

【００６５】アクセス・キーを受け取ったクライアントは、アクセス・キーに対して後に変更を加えることに備えて、サーバの公開鍵ｐｋｅｙも取得しておく。

【００６６】１．３　新たなアクセス・キーの生成

クライアントは、さらに別のクライアントにアクセス・キーを委譲したいことがある。例えば、あるクライアン

トＡは、自分の不在中に別のクライアントＢにオブジェクトの管理を委ねたいときにはアクセス・キーを渡しておけばよい。

【００６７】ところが、自分と同じ権限情報を持つアクセス・キーをクライアントＢに渡してしまったならば、思わぬ不利益を被ることがある。例えば、同じ有効期限のままでアクセス・キーを渡してしまっては、復帰後もクライアントＢがオブジェクトにアクセスし続けることができる。また、クライアントＢはオブジェクトの読み出しオペレーションだけを許可すれば充分なのに、クライアントＡと等しく書き込みや実行オペレーションまで許可してしまっては、オブジェクトのセキュリティは脅かされかねない。すなわち、クライアントＡは、自分と同じ権限を与えてもよいとは限らず、権限を弱めなければならない場合もある。例えばアクセス・キーの有効期限を制限するとか、操作権限を読み出しに限定して書き込みや実行を禁止する等である。

【００６８】このような場合、クライアントは、他のクライアントに与えてもよいケイパビリティを自ら作成する。これを第２の権限情報P_2としておく。そして、クライアントは、第１のアクセス・キーｐｋｅｙ（P_1，＊ａ）と第２の権限情報P_2を連結（例えばビット連結）し、さらに公開鍵ｐｋｅｙを適用することで第２のアクセス・キーｐｋｅｙ（P_2，ｐｋｅｙ（P_1，ａ））を生成する。

【００６９】第２のアクセス・キーは、公開鍵ｐｋｅｙで暗号化されているので、第２の権限情報Ｐ２を作成したクライアント自身と、秘密鍵ｓｋｅｙを持つサーバ以外は、第２のアクセス・キーに含まれた権限情報P_2の内容を解読できない。例えば第２のアクセス・キーを譲り受けたクライアントも、基本的には、自分に与えられた権限情報P_2を確認できない。

【００７０】以下では、アクセス識別子ａから第Ｎ番目に派生したアクセス・キーのことを「第Ｎのアクセス・キー」ａｋｅｙ$_N$と呼び、また、第Ｎ番目のアクセス・キーａｋｅｙ$_N$に与えられた権限情報を第Ｎの権限情報P_Nと呼ぶことにする（但し、Ｎは０以上の整数であり、第０のアクセス・キーはアクセス識別子ａとする）。第Ｎのアクセス・キーと第Ｎ－１のアクセス・キーの間には、下式の関係が成立する。

【００７１】

【数１】

$$akey_N = pkey(P_N, akey_{N-1})$$

【００７２】１．４　オブジェクトへのアクセス

第Ｎのアクセス・キーａｋｅｙ$_N$を持つクライアントは、オブジェクトＡを管理するアクセス管理サーバに対して、このアクセス・キーを用いてオブジェクトＡへのアクセスを要求することができる。アクセス要求は、アクセス・キーを含んだ要求メッセージの形式で送信される。

【００７３】これに対し、アクセス管理サーバは、アクセス・キーａｋｅｙＮが正当なものがどうかを検証しなければならない。

【００７４】アクセス管理サーバは、要求メッセージを受信すると、その中に含まれるアクセス・キーａｋｅｙ$_N$を取り出す。そして、サーバ自身が持つ公開鍵暗号系の秘密鍵ｓｋｅｙを用いてこのアクセス・キーを復元する。上式がａｋｅｙ$_N$＝ｐｋｅｙ（P_N，ａｋｅｙ$_{N-1}$）成立することから、この復元作業によって、第Ｎの権限情報ＰＮと第Ｎ－１番目のアクセス・キーａｋｅｙ$_{N-1}$が得られる。

【００７５】アクセス管理サーバは、得られたアクセス・キーａｋｅｙ$_{N-1}$が保管しているアクセス識別子ａと一致すれば、復元処理を終了する。一致しなければ、さらに秘密鍵ｓｋｅｙを用いた復元処理を試みる。このような復元処理は、アクセス・キーａｋｅｙ$_{N-1}$とアクセス識別子ａとの照合が成功裏に終わるまで再帰的に試行される。

【００７６】再帰的な復元処理の結果、アクセス管理サーバは、一連の権限情報P_N，P_{N-1}，…，P_2，P_1も得る。アクセス管理サーバは、この一連の権限情報のコンテキストを検証してもよい。アクセス管理サーバは、例えば、アクセス・キーを作成する各クライアントに対して、権限を弱める方向でしか権限情報の作成を認めないように規定することができる。権限を弱めるとは、例えばアクセス回数を減らすとか、有効期限を短縮するとか、操作を制限することを意味する。あるいは、アクセス回数のみ権限の強化を認める、などのようにコンテキストを規定してもよい。

【００７７】一連の権限情報のコンテキストを検証した結果、コンテキストが所定の規則に反していれば、アクセス管理サーバは、要求メッセージ中のアクセス・キーａｋｅｙ$_N$を不正とみなすこともできる。

【００７８】アクセス管理サーバは、アクセス・キーとオブジェクトＡのアクセス識別子との照合と、権限情報のコンテキスト検証に成功したときのみ、要求メッセージ中のアクセス・キーａｋｅｙ$_N$が正当であると判断する。そして、該当するオブジェクトＡへのアクセスを認める。

【００７９】１．５　アクセス・キーの無効化

アクセス管理サーバは、一度正当なものとして認められたアクセス・キーを無効化する機構を備えてもよい。この機構は、無効化されたアクセス・キーを登録するための無効アクセス・キー・テーブルを備えることで実現される。

【００８０】クライアントは、無効化したいアクセス・キーを含めた無効化要求メッセージを送信する。アクセ

ス管理サーバは、無効化要求メッセージを受信すると、アクセス・キーを取り出して、これを無効アクセス・キー・テーブルに追加登録すればよい。

【００８１】アクセス管理サーバは、オブジェクトＡへのアクセス要求メッセージを受信すると、アクセス・キーを取り出し、秘密鍵ｓｋｅｙを用いてアクセス・キーを再帰的に復元していく（上述）。この再帰的な復元工程の途中で、無効アクセス・キー・テーブルに登録されているアクセス・キーと同じアクセス・キーが出現すると、要求メッセージが不正であると判断して、該当するオブジェクトＡへのアクセスを拒否する。

【００８２】２．第２の実施形態

第１の実施形態では、アクセス・キーを生成するために、アクセス管理サーバが持つ公開鍵暗号系の公開鍵と暗号鍵を用いた。第２の実施形態では、暗号鍵の代わりに２個の引数を持つ一方向性関数を用いることにする。ここで言う「一方向性関数」とは、逆関数を求めることが極めて困難な関数のことであり、該関数を適用する前の引数の値を推測することを不可能にする作用がある。アクセス管理サーバとクライアントは２引数（ｘ，ｙ）の一方向性関数ｆ（ｘ，ｙ）を共有するものとする。

【００８３】２．１　アクセス管理サーバでの操作

アクセス管理サーバは、まず、あるオブジェクトＡへのアクセスを許可するためのアクセス識別子ａを生成する。

【００８４】また、アクセス管理サーバは、アクセス識別子ａに対して第１の権限情報P_1を生成する。アクセス管理サーバは、アクセス識別子を権限情報と対応付けて保管する。第１の権限情報P_1とは、アクセス識別子ａを提示したものに与えられる権限すなわちケイパビリティのことである（前述）。

【００８５】次いで、アクセス管理サーバは、アクセス識別子ａと第１の権限情報P_1に一方向性関数ｆを適用して、第１のアクセス・キーｆ（P_1，ａ）を生成する。アクセス管理サーバは、第１のアクセス・キーｆ（P_1，ａ）を、オブジェクトＡと対応付けて保管しておく。

【００８６】２．２　クライアントでの操作

生成された第１のアクセス・キーｆ（P_1，ａ）は、例えばネットワーク経由で、オブジェクトＡへのアクセスが許されたクライアントに送信される。正当なアクセス・キーｆ（P_1，ａ）を持つクライアントは、これを提示することでオブジェクトＡへのアクセスが許される。

【００８７】アクセス・キーを受け取ったクライアントは、アクセス・キーの権限情報に対して後で変更を加えることに備えて、アクセス管理サーバが使用する一方向性関数も取得しておく。

【００８８】２．３　新たなアクセス・キーの生成

クライアントは、さらに別のクライアントにアクセス・キーを委譲したいことがある（上述）。

【００８９】このような場合、クライアントは、他のクライアントに与えてもよいケイパビリティを自ら作成する。これを第２の権限情報P_2としておく。そして、クライアントは、第１のアクセス・キーｆ（P_1，ａ）と第２の権限情報P_2に対してさらに一方向性関数ｆを適用して、第２のアクセス・キーｆ（P_2，ｆ（P_1，ａ））を生成する。

【００９０】一方向性関数ｆのパラメータ値は、アクセス管理サーバも解読できない。このため、第２のアクセス・キーに第２の権限情報P_2を添付して第２のアクセス・キーを委譲するようにする。

【００９１】以下では、アクセス識別子ａから第Ｎ番目に派生したアクセス・キーのことを「第Ｎのアクセス・キー」ａｋｅｙ$_N$と呼び、また、第Ｎ番目のアクセス・キーａｋｅｙ$_N$に与えられた権限情報を第Ｎの権限情報P_Nと呼ぶことにする（但し、Ｎは０以上の整数であり、第０のアクセス・キーはアクセス識別子ａとする）。第Ｎのアクセス・キーと第Ｎ－１のアクセス・キーの間には、下式の関係が成立する。

【００９２】

【数２】

$$akey_N = f(P_N, akey_{N-1})$$

【００９３】一方向性関数ｆを一度適用すると、権限情報P_Nは解読不能となってしまう。このため、アクセス・キーを作成したクライアントは、権限情報P_Nを添えてアクセス・キーｆ（P_N，ａｋｅｙ$_{N-1}$）を配布するようにする。この結果、第Ｎのアクセス・キーを送信するメッセージ中には、アクセス・キーに含まれる全ての権限情報P_1，P_2，…，P_{N-1}，P_Nが同封されることになる。

【００９４】２．４　オブジェクトへのアクセス

第Ｎのアクセス・キーａｋｅｙ$_N$を持つクライアントは、オブジェクトＡを管理するアクセス管理サーバに対して、このアクセス・キーを用いてオブジェクトＡへのアクセスを要求することができる。

【００９５】但し、アクセス管理サーバは一方向性関数ｆを適用された第Ｎのアクセス・キーａｋｅｙ$_N$を解読できない。このため、クライアントは、アクセス・キーａｋｅｙ$_N$を受信したときに添付されていた全ての権限情報P_1，P_2，…，P_{N-1}，P_Nを沿えて、要求メッセージの形式で送信する。

【００９６】これに対し、アクセス管理サーバは、アクセス・キーａｋｅｙ$_N$が正当なものがどうかを検証を行う。

【００９７】アクセス管理サーバは、要求メッセージを受信すると、その中に含まれるアクセス・キーａｋｅｙ$_N$と全ての権限情報P_1，P_2，…，P_{N-1}，P_Nを取り出す。そして、一方向性関数ｆを用いて、第１のアクセス・キーａｋｅｙ$_1$（＝ｆ（P_1，ａ）），第２のアクセス

・キーａｋｅｙ$_2$（＝ｆ（P_2，ｆ（P_1，ａ））），…，第Ｎのアクセス・キーａｋｅｙ$_N$（＝ｆ（P_N，ａｋｅｙ$_{N-1}$））を順次生成していく。

【００９８】そして、アクセス管理サーバは、自ら生成した第Ｎのアクセス・キーａｋｅｙ$_N$が、要求メッセージに含まれていたアクセス・キーａｋｅｙ$_N$と一致すれば、アクセス・キーの照合は成功したと判断する。

【００９９】また、アクセス管理サーバは、要求メッセージに含まれている一連の権限情報についてのコンテキストの検証（上述）を行ってもよい。

【０１００】アクセス管理サーバは、アクセス・キーａｋｅｙ$_N$の検査と、権限情報のコンテキスト検証に成功したときのみ、要求メッセージ中のアクセス・キーａｋｅｙ$_N$が正当であると判断する。そして、対応するオブジェクトへのアクセスを認める。

【０１０１】２．５　アクセス・キーの無効化

アクセス管理サーバは、一度正当なものとして認められたアクセス・キーを無効化する機構を備えてもよい。この機構は、無効化されたアクセス・キーを登録するための無効アクセス・キー・テーブルを備えることで実現される。

【０１０２】クライアントは、無効化したいアクセス・キーを含めた無効化要求メッセージを送信する。アクセス管理サーバは、無効化要求メッセージを受信すると、＊アクセス・キーを取り出して、これを無効アクセス・キー・テーブルに追加登録すればよい。

【０１０３】アクセス管理サーバは、オブジェクトＡへのアクセス要求メッセージを受信すると、アクセス・キーとａｋｅｙ$_N$と全ての権限情報P_1，P_2，…，P_{N-1}，P_Nを取り出す。そして、一方向性関数ｆを用いて、第１のアクセス・キーａｋｅｙ$_1$（＝ｆ（P_1，ａ）），第２のアクセス・キーａｋｅｙ$_2$（＝ｆ（P_2，ｆ（P_1，ａ））），…，第ＮのアクセスキーａｋｅｙＮ（＝ｆ（P_N，ａｋｅｙ$_{N-1}$））を順次生成していく（上述）。

【０１０４】このアクセス・キーの生成工程の途中で、無効アクセス・キー・テーブルに登録されているアクセス・キーが出現すると、要求メッセージが不正であると判断して、該当するオブジェクトＡへのアクセスを拒否する。

【０１０５】３．第３の実施形態

第２の実施形態では、アクセス・キーを生成するために、２個の引数を持つ一方向性関数を用いた。第３の実施形態では、この一方向性関数が可換であるとする。可換な一方向性関数とは、下式が成立する一方向性関数のことである。

【０１０６】

【数３】

$$f(x, f(y, a)) = f(y, f(x, a))$$

【０１０７】アクセス管理サーバとクライアントは可換な一方向性関数ｆ（ｘ，ｙ）を共有するものとする。

【０１０８】３．１　アクセス管理サーバでの操作

アクセス管理サーバは、まず、あるオブジェクトＡへのアクセスを許可するためのアクセス識別子ａを生成する。

【０１０９】また、アクセス管理サーバは、アクセス識別子ａに対して第１の権限情報P_1を生成する。アクセス管理サーバは、アクセス識別子を権限情報と対応付けて保管する。第１の権限情報P_1とは、アクセス識別子ａを提示したものに与えられる権限すなわちケイパビリティのことである（前述）。

【０１１０】次いで、アクセス管理サーバは、アクセス識別子ａと第１の権限情報P_1に可換な一方向性関数ｆを適用して、第１のアクセス・キーｆ（P_1，ａ）を生成する。アクセス管理サーバは、第１のアクセス・キーｆ（P_1，ａ）を、オブジェクトＡと対応付けて保管しておく。

【０１１１】３．２　クライアントでの操作

生成された第１のアクセス・キーｆ（P_1，ａ）は、例えばネットワーク経由で、オブジェクトへのアクセスが許されたクライアントに送信される。正当なアクセス・キーｆ（P_1，ａ）を持つクライアントは、これを提示することでオブジェクトＡへのアクセスが許される。

【０１１２】アクセス・キーを受け取ったクライアントは、アクセス・キーの権限情報に対して後で変更を加えることに備えて、アクセス管理サーバが使用する可換な一方向性関数ｆも取得しておく。

【０１１３】３．３　新たなアクセス・キーの生成

クライアントは、さらに別のクライアントにアクセス・キーを委譲したいことがある（上述）。

【０１１４】このような場合、クライアントは、他のクライアントに与えてもよいケイパビリティを自ら作成する。これを第２の権限情報P_2としておく。そして、クライアントは、第１のアクセス・キーｆ（P_1，ａ）と第２の権限情報P_2に対してさらに可換な一方向性関数ｆを適用して、第２のアクセス・キーｆ（P_2，ｆ（P_1，ａ））を生成する。

【０１１５】可換な一方向性関数ｆのパラメータ値は、アクセス管理サーバも解読できない。このため、第２のアクセス・キーに第２の権限情報P_2を添付して第２のアクセス・キーを委譲するようにする。

【０１１６】以下では、アクセス識別子ａから第Ｎ番目に派生したアクセス・キーのことを「第Ｎのアクセス・キー」ａｋｅｙ$_N$と呼び、また、第Ｎ番目のアクセス・キーａｋｅｙ$_N$に与えられた権限情報を第Ｎの権限情報P_Nと呼ぶことにする（但し、Ｎは０以上の整数であり、第０のアクセス・キーはアクセス識別子ａとす

る）。第Ｎのアクセス・キーと第Ｎ－１のアクセス・キーの間には、下式の関係が成立する。

【０１１７】

【数４】

$$akey_N = f(P_N, akey_{N-1})$$

【０１１８】可換な一方向性関数ｆを一度適用すると、権限情報P_Nは解読不能となってしまう。このため、アクセス・キーを作成したクライアントは、権限情報P_Nを添えてアクセス・キーｆ（P_N，$akey_{N-1}$）を配布するようにする。この結果、第Ｎのアクセス・キーを送信するメッセージ中には、アクセス・キーに含まれる全ての権限情報P_1，P_2，…，P_{N-1}，P_Nが同封されることになる。

【０１１９】３．４　オブジェクトへのアクセス

第Ｎのアクセス・キー$akey_N$を持つクライアントは、オブジェクトＡを管理するアクセス管理サーバに対して、このアクセス・キーを用いてオブジェクトＡへのアクセスを要求することができる。

【０１２０】但し、アクセス管理サーバは可換な一方向性関数ｆを適用された第Ｎのアクセス・キー$akey_N$を解読できない。このため、クライアントは、アクセス・キー$akey_N$を受信したときに添付されていた全ての権限情報P_1，P_2，…，P_{N-1}，P_Nを沿えて、要求メッセージの形式で送信する。

【０１２１】これに対し、アクセス管理サーバは、アクセス・キー$akey_N$が正当なものがどうかを検証を行う。

【０１２２】アクセス管理サーバは、要求メッセージを受信すると、その中に含まれるアクセス・キー$akey_N$と全ての権限情報P_1，P_2，…，P_{N-1}，P_Nを取り出す。そして、可換な一方向性関数ｆを用いて、各アクセス・キーを自ら生成する。但し、可換な一方向性関数ｆは順序性を守る必要がないので、各アクセス・キーを任意の順番で生成することができる。

【０１２３】そして、アクセス管理サーバは、自ら生成した第Ｎのアクセス・キー$akey_N$が、要求メッセージに含まれていたアクセス・キー$akey_N$と一致すれば、アクセス・キーの照合は成功したと判断する。

【０１２４】また、アクセス管理サーバは、要求メッセージに含まれている一連の権限情報についてのコンテキストの検証（上述）を行ってもよい。

【０１２５】アクセス管理サーバは、アクセス・キー$akey_N$の検査と、権限情報のコンテキスト検証に成功したときのみ、要求メッセージ中のアクセス・キー$akey_N$が正当であると判断する。そして、該当するオブジェクトＡへのアクセスを認める。

【０１２６】なお、第３の実施形態でも、第１及び第２の実施形態と同様にアクセス・キーを無効化するための機構を備えていてもよい。但し、第２の実施形態と略同一の仕組みにより実現できるので、ここでは敢えて説明しない。

【０１２７】

【実施例】以下、図面を参照しながら本発明の実施例を詳解する。

【０１２８】図１には、本発明の実施に供されるネットワーク・システム１００の構成を模式的に示している。同図に示すように、ネットワーク・システム１００は、データの伝送媒体であるネットワーク１０上に、複数のコンピュータ・システム５０Ａ，５０Ｂ，…が接続されて構成される。

【０１２９】ネットワーク１０は、例えば大学や企業の構内などの限られた空間内に敷設されたＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）である。あるいは、ＬＡＮ同士を専用線等で相互接続してなるＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）や、一般公衆回線（ＰＳＴＮ：Ｐｕｂｌｉｃ　Ｓｗｉｔｃｈｅｄ　Ｔｅｌｅｐｈｏｎｅ　Ｎｅｔｗｏｒｋ）、ＩＳＤＮ（Ｉｎｔｅｇｒａｔｅｄ　Ｓｅｒｖｉｃｅ　Ｄｉｇｉｔａｌ　Ｎｅｔｗｏｒｋ）、これらネットワークの大規模な集合体であるインターネットであってもよい。ネットワーク１０は、主として、接続された各コンピュータ・システム５０Ａ，５０Ｂ，…においてアプリケーションを分散処理する分散型ネットワークである。

【０１３０】各コンピュータ・システム５０Ａ，５０Ｂ，…は、ＬＡＮアダプタやモデム、ＴＡ（Ｔｅｒｍｉｎａｌ　Ａｄａｐｔｅｒ）等の回線終端装置（ＤＣＥ：Ｄａｔａ　Ｃｉｒｃｕｉｔ　Ｔｅｒｍｉｎａｔｉｎｇ　Ｅｑｕｉｐｍｅｎｔ）を介してネットワーク１０に接続されている。各コンピュータ・システム５０Ａ，５０Ｂ，…は、オブジェクトを所有するオブジェクト・サーバと、オブジェクトへのアクセスを要求するオブジェクト・クライアントに２分される。サーバ又はクライアントの機能に特化してデザインされた専用マシンであってもよいが、一般には、サーバ用又はクライアント用のアプリケーションを導入して動作する汎用機でよい。各コンピュータ・システム５０Ａ，５０Ｂ，…同士は、ネットワーク１０を介して、例えばＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　ＣｏｎｔｒｏｌＰｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）接続されている。

【０１３１】オブジェクト・サーバ５０Ａ，５０Ｂは、複数のオブジェクトを所有する。オブジェクトの一例は、ホームページを形成するためのＨＴＭＬ（Ｈｙｐｅｒｔｅｘｔ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）ファイルである。ＨＴＭＬファイルは、ＨＴＴＰ（Ｈｙｐｅｒｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）プロトコルに従ってネットワーク１０上を伝送することができることから、以下では「ＨＴＴＰオブジェクト」と呼ぶことにする。一方のオブジェクト・クライアント５０

C，５０D，５０Eは、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）の形式でＨＴＴＰオブジェクトの場所を指定することができる。

【０１３２】また、ネットワーク上には、さらにＨＴＴＰオブジェクトへのアクセス管理（すなわちオブジェクトのセキュリティ）管理を行うためのアクセス管理サーバも存在する。ネットワーク１０上の別のコンピュータ・システムがアクセス管理サーバとして働くことも可能であるが、オブジェクト・サーバ自身がアクセス管理機能を持つことも可能である。後述の各実施例では、オブジェクト・サーバ内の「プロキシ・オブジェクト」がＨＴＴＰオブジェクトへのアクセス管理を行うものとする。

【０１３３】図２には、ＨＴＴＰオブジェクト・サーバ５０Ａの構成を模式的に示している。図示しない他のオブジェクト・サーバ５０Ｂも同様の構成を備えていると把握されたい。同図に示すように、オブジェクト・サーバ５０Ａは、Ｎ個のＨＴＴＰオブジェクト３２１～３２Ｎの他、各ＨＴＴＰオブジェクトへのアクセスを管理するプロキシ・オブジェクト３０１を含んでいる。オブジェクト・サーバ５０ＡのＵＲＬは、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）を用いたＨＴＴＰプロトコルに従って”ｈｔｔｐｓ：／／ｗｗｗ３００／”と表されるものとする。（以下の実施例では、ケイパビリティのような秘密情報をネットワーク経由で安全に移送するために、ＳＳＬを用いているが、一般には、暗号化を行う他の通信方式、又は、暗号化を行わない通信方式を用いても、本発明の効果を奏することはできる。）

【０１３４】プロキシ・オブジェクト３０１は、各ＨＴＴＰオブジェクトに対するリファレンスすなわちアクセス識別子を生成する。１つのＨＴＴＰオブジェクトに対して２以上のアクセス識別子を生成してもよい。同一のＨＴＴＰオブジェクトに対する各アクセス識別子には、それぞれ個別にアクセス権限すなわちケイパビリティ（Ｃａｐａｂｉｌｉｔｙ）が与えられる。プロキシ・オブジェクト３０１は、個々のアクセス権限を管理するために、アクセス識別子毎にアクセス権限保持部を生成する。

【０１３５】図２に示した例では、あるＨＴＴＰオブジェクト３９１に対して、少なくとも２つのアクセス識別子が生成されており、プロキシ・オブジェクト３０１は各アクセス識別子に対してそれぞれアクセス権限保持部３１１及び３１Ｍを生成している。

【０１３６】アクセス権限保持部３１１は、アクセス識別子保持部３２１と、ケイパビリティ・リスト保持部３３１と、無効リスト保持部３４１と、リファレンス保持部３５１とを含んでいる。他のアクセス権限保持部３１Ｍ…も、アクセス権限保持部３１１と略同一の構成を有すると把握されたい。

【０１３７】アクセス識別子保持部３１１は、与えられたアクセス識別子を記憶するユニットである。リファレンス保持部３５１は、アクセス識別子に対応するＨＴＴＰオブジェクト３９１へのポインタを記憶するユニットである。

【０１３８】アクセス識別子には、該当するＨＴＴＰオブジェクトに対する権限が規定されている。ここで言う権限とは、ＨＴＴＰオブジェクトに対する操作権限（例えば読み出しのみ、読み書き可、実行可）や、アクセス有効期限、有効アクセス回数などである。これらの権限情報は「ケイパビリティ」と呼ばれる。ケイパビリティは、原初的にはプロキシ・オブジェクト３０１が与えるが、後述するようにアクセス・キーを付与されたＨＴＴＰクライアントが逐次作成する。ケイパビリティ・リスト保持部３３１は、１つのアクセス識別子から派生した各ケイパビリティの現在の権限内容を保管するユニットである。

【０１３９】また、アクセス・キーを生成した（又は受け取った）クライアントは、アクセス・キーを無効化することが許容されている。無効リスト保持部３４１は、１つのアクセス識別子から派生したアクセス・キーのうち無効化されたものを保管するユニットである。

【０１４０】プロキシ・オブジェクト３０１内で生成されたアクセス権限保持部３１１，…，３１Ｍは、１つのアクセス権限集合３０２を構成する。

【０１４１】本実施例では、ＵＲＬを用いてケイパビリティを表現するとともに、暗号を用いてＵＲＬを推測困難な形式に変換することによって、ＨＴＴＰオブジェクトに対するアクセス保護を実現する。以下、各実施例について説明する。

【０１４２】１．第１の実施例

第１の実施例では、各アクセス識別子に関する権限情報のセキュリティを守るために、プロキシ・オブジェクト３０１が保有する公開鍵暗号系の公開鍵ｐｋｅｙと秘密鍵ｓｋｅｙを用いる。

【０１４３】プロキシ・オブジェクト３０１は、アクセス識別子ａとこれに対する権限情報Ｐ１を生成する。さらに、プロキシ・オブジェクト３０１は、権限情報P_1とアクセス識別子を連結して、公開鍵ｐｋｅｙで暗号化することによって、アクセス・キー$akey_1 = pkey(P_1 . a)$を生成する。

【０１４４】ＨＴＴＰクライアント５０Ｃは、ＨＴＴＰサーバ３００との間で、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）などの暗号を用いたメッセージ交換により、アクセス・キー$akey_1$を受信する。

【０１４５】アクセス・キー$akey_1$を受信したＨＴＴＰクライアント５０Ｃは、自身が作成した権限情報”ＧＥＴ，２，Ａｐｒ：２４：１０：００：４８：１９９８：ＧＭＴ，Ａｐｒ：２４：１０：０５：４８：１９９８：ＧＭＴ”と、自身が発生した乱数Ｒｎｄ１を連結し、さらにこれを公開鍵ｐｋｅｙで暗号化することで、

下式［数５］に示すアクセス・キーａｋｅｙ₂を生成する。但し、権限内容には、実行することができるメソッドの他に、使用可能な記憶容量の上限やプロセッサ占有時間の上限を含んでいてもよい。また、権限情報を記述＊するために、他の任意の表現形式を用いてもよい。

【０１４６】

【数５】

$$\{akey_1, GET,2,Apr:24:10:00:48:1998:GMT,Apr:24:10:05:48:1998:GMT,Rnd1\}pkey$$

【０１４７】アクセス・キーａｋｅｙ₂は、ａｋｅｙ₁と結び付けられたオブジェクトに対して、世界時で１９９８年の４月２４日１０時０分４８秒から１０時５分４８秒の間にＧＥＴメソッドを２回実行することを許容する旨の権限情報を包含している。

※【０１４８】次いで、ＨＴＴＰクライアント５０Ｃは、アクセス・キーａｋｅｙ₂を用いて下式［数６］に示すＵＲＬを生成する。

【０１４９】

【数６】

$$http://www300/\{akey_1, GET,2,Apr:24:10:00:48:1998:GMT,Apr:24:10:05:48:1998:GMT,Rnd1\}pkey$$

【０１５０】そして、ＨＴＴＰクライアント５０Ｃは、他のＨＴＴＰクライアント５０ＤにこのＵＲＬを送信する。

【０１５１】ＨＴＴＰクライアント５０Ｄは、このＵＲＬに基づき、ネットワーク１０上のｗｗｗ３００で指定されるホスト（この例ではプロキシ・オブジェクト３０★１が存在するサーバと同一）で動作しているＨＴＴＰサーバ３００と、ＳＳＬを用いて接続し、下式［数７］で示したメッセージを送信する。

【０１５２】

【数７】

$$GET\{akey_1, GET,2,Apr:24:10:00:48:1998:GMT,Apr:24:10:05:48:1998:GMT,Rnd1\}pkey \quad HTTP/1.1$$

【０１５３】ＨＴＴＰサーバ３００は、このメッセージを受信すると、メッセージからメソッドＧＥＴと、アクセス・キーａｋｅｙ₂２に相当する文字列”ａｋｅｙ１，ＧＥＴ，２，Ａｐｒ：２４：１０：００：４８：１９９８：ＧＭＴ，Ａｐｒ：２４：１０：０５：４８：１９９８：ＧＭＴ，Ｒｎｄ１”を抽出して、プロキシ・オブジェクト３０１に入力する。

【０１５４】プロキシ・オブジェクト３０１は、自身の秘密鍵ｓｋｅｙを適用して復号化した結果から、アクセス・キーａｋｅｙ₂に与えられたケイパビリティが「ａｋｅｙ₁と結び付けられたオブジェクトに対して、世界時で１９９８年の４月２４日１０時０分４８秒から１０☆時５分４８秒の間にＧＥＴメソッドを２回実行することの権利」であることを判読する。

【０１５５】また、プロキシ・オブジェクト３０１は、世界時での現在時刻を取得する。例えば現在時刻が１９９８年４月２４日１０時１分４８秒であれば、ケイパビリティ・リスト保持部３３１に下式［数８］に示す内容のケイパビリティを保存するとともに、アクセス・キーに結び付けられたＨＴＴＰオブジェクト３９１に対してメッセージＧＥＴを送信する。

【０１５６】

【数８】

$$\begin{aligned}&メソッド：GET\\&残り回数：1\\&有効期限：Apr:24:10:00:48:1998:GMT,Apr:24:10:05:48:1998:GMT\\&アクセス・キー：akey_1, GET,2,Apr:24:10:00:48:1998:GMT,Apr:24:10:05:48:1998:GMT,Rnd1,pkey\end{aligned}$$

【０１５７】ここで、さらにＨＴＴＰクライアント５０ＤがＨＴＴＰサーバ３００に対して［数７］で示したものと同一のメッセージを送信したときの動作について考察してみる。

【０１５８】ＨＴＴＰサーバ３００は、メッセージを受信すると、メッセージからメソッドＧＥＴと、アクセス・キーａｋｅｙ₂に相当する文字列”ａｋｅｙ１，ＧＥＴ，２，Ａｐｒ：２４：１０：００：４８：１９９８：ＧＭＴ，Ａｐｒ：２４：１０：０５：４８：１９９８：ＧＭＴ，Ｒｎｄ１”を抽出して、プロキシ・オブジェクト３０１に入力する。

【０１５９】プロキシ・オブジェクト３０１は、アクセス権限集合３０２に登録されているアクセス・キーを検索して、アクセス・キーａｋｅｙ₂と同一のキーが既に登録されているかどうかを判断する。そして、このアクセス・キーａｋｅｙ₂に該当するケイパビリティの現在の内容が以下の［数９］の通りであることを、ケイパビリティ・リスト保持部３３１から導出する。

【０１６０】

【数９】

33 34

メ ソ ッ ド：GET
残 り 回 数：１
有 効 期 限：Apr.24:10:00:48:1998:GMT,Apr.24:10:05:48:1998:GMT
アクセス・キー：$akey_1$, GET,2,Apr.24:10:00:48:1998:GMT,Apr.24:10:05:48:1998:GMT,Ｒｎｄ１,pkey

【０１６１】プロキシ・オブジェクト３０１は、世界時での現在時刻を取得する。例えば現在時刻が１９９８年４月２４日１０時3分４８秒でれあば、ケイパビリティ・リスト保持部３３１中の当該エントリの内容を以下の通りに変更した後、ＨＴＴＰオブジェクト３９１に対し＊てメッセージＧＥＴを送信する。ここで行われるケイパビリティの変更内容は、残り回数を１だけ減分することである。

【０１６２】
【数１０】

メ ソ ッ ド：GET
残 り 回 数：０
有 効 期 限：Apr.24:10:00:48:1998:GMT,Apr.24:10:05:48:1998:GMT
アクセス・キー：$akey_1$, GET,2,Apr.24:10:00:48:1998:GMT,Apr.24:10:05:48:1998:GMT,Ｒｎｄ１,pkey

【０１６３】この後、プロキシ・オブジェクト３０１は、世界時での現在時刻が１０時５分４８秒を経過した時点で、ケイパビリティ・リスト保持部３３１中の当該エントリを削除する（削除しないまでも、エントリに対応するケイパビリティは失効する）。

【０１６４】２．第２の実施例
第２の実施例では、各アクセス識別子に関する権限情報のセキュリティを守るために、プロキシ・オブジェクト３０１が保有する一方向性関数ｆを用いる。「一方向性関数」とは、逆関数を求めることが極めて困難な関数のことであり、該関数を適用する前の引数の値を推測することを不可能にする作用がある。この実施例で用いる一方向性関数は可換であってもよい。

【０１６５】プロキシ・オブジェクト３０１は、ＨＴＴＰオブジェクト３９１の１つのリファレンスに対して、※アクセス識別子ａを生成し、これをアクセス識別子３２１で保存する。

【０１６６】プロキシ・オブジェクト３０１は、次いで、ケイパビリティ識別子Ｒｎｄ０を生成し、ケイパビリティ・リスト保持部３３１でこれを保存する。

【０１６７】さらに、ケイパビリティ・オブジェクト３０１は、ＨＴＴＰクライアントにＨＴＴＰオブジェクトへのアクセス（操作）を許可する権限内容を記述した権限情報ｒｉｇｈｔ１とケイパビリティ識別子Ｒｎｄ０に対して一方向性関数ｆを適用して、下式［数１１］に示すようなケイパビリティｃａｐ１を生成する。ｃａｐ１は、２項の組のビット列として表される。

【０１６８】
【数１１】

$$cap1 = (f(Rnd0, right1, Rnd1), ((right1, Rnd1)))$$

【０１６９】上式の２項組の第１項は権限情報の不正な改竄を防止するためのチェック・フィールドとして機能し、また、第２項は権限の変更履歴をリスト状に記述している。

【０１７０】上式に含まれる権限情報ｒｉｇｈｔ１は、世界時で１９９８年4月２４日０時０分０秒から４月２★５日０時０分０秒の間に、ＧＥＴメソッドを５回実行することを許容する旨を示すものであり、以下の［数１２］で示した文字列で構成されているものとする。

【０１７１】
【数１２】

(GET,5,Apr:24:00:00:00:1998:GMT,Apr:25:00:00:00:1998:GMT)

【０１７２】但し、権限内容ｒｉｇｈｔ１には、実行することができるメソッドの他に、使用可能な記憶容量の上限やプロセッサ占有時間の上限を含んでいてもよい。また、権限情報を記述するために、他の任意の表現形式を用いてもよい。

【０１７３】次いで、プロキシ・オブジェクト３０１は、サーバ名とアクセス識別子とケイパビリティを含んだ以下の［数１３］に示すＵＲＬ文字列を生成して、ＨＴＴＰクライアント５０Ｃに送信する。

【０１７４】
【数１３】

https://www300/a/cap1/

【０１７５】ＨＴＴＰクライアント５０Ｃは、ＨＴＴＰサーバ３００との暗号を用いたメッセージ交換により、ケイパビリティｃａｐ１を含むＵＲＬを受信する。

【０１７６】以下では、ＨＴＴＰクライアント５０Ｃが、ＨＴＴＰサーバ３００から取得した権限を弱めて他のＨＴＴＰ５０Ｄに委譲する操作について説明する。

【０１７７】ＨＴＴＰクライアント５０Ｃは、以下の［数１４］に示す新しいｒｉｇｈｔ２と、ケイパビリティ識別子Ｒｎｄ２を生成する。

【０１７８】
【数１４】

35　　36

(GET, 2, Apr.24:10:00:48:1998:GMT,Apr.24:10:05:48:1998:GMT)

【０１７９】上記の権限情報ｒｉｇｈｔ２は、世界時で１９９８年4月２４日１０時0分４８秒から１０時５分４８秒までの間に、ＧＥＴメッセージを２回実行することができる権限を記述している。ＨＴＴＰクライアント５０Ｃは、一方向性関数ｆを用いて、２項組を表すビット列として下式［数１５］のようなケイパビリティｃａｐ２を生成する。

【０１８０】

【数１５】

$$cap2 = (f(cap1, right1, Rnd2), ((right1, Rnd1), (right2, Rnd2)))$$

【０１８１】次いで、ＨＴＴＰクライアント５０Ｃは、ｃａｐ２を基に、以下のよ［数１６］に示すようなＵＲＬ文字列を生成して、これを他のＨＴＴＰクライアント５０Ｄに送信する。

【０１８２】

【数１６】

https://www300/a/ｃａｐ２

【０１８３】ＨＴＴＰクライアント５０Ｄは、ＨＴＴＰクライアント５０Ｃから受信したＵＲＬに従って、ネットワーク上においてｗｗｗ３００で表されるホストで動作中のＨＴＴＰサーバ３００とＳＳＬを用いて接続して、以下の［数１７］に示すメッセージを送信する。

【０１８４】

【数１７】

GET /a/ｃａｐ２ HTTP/1.1

【０１８５】ＨＴＴＰサーバ３００は、メッセージを受信すると、このメッセージの中から、ＧＥＴメソッドと、アクセス識別子ａと、ケイパビリティｃａｐ２を抽出する（ケイパビリティｃａｐ２は、［数１５］に示した文字列で構成される）。そして、ＨＴＴＰサーバ３００は、これらのパラメータをプロキシ・オブジェクト３０１に入力する。

【０１８６】プロキシ・オブジェクト３０１は、アクセス権限集合３０２の中で入力されたアクセス識別子ａを検索して、該当するアクセス権限保持部３１１内のケイパビリティ・リスト保持部３３１が保持しているケイパビリティ識別子Ｒｎｄ０を取得する。

【０１８７】次いで、プロキシ・オブジェクト３０１は、以下のような《処理手順１》を実行する。

【０１８８】

【数１８】

《処理手順１》

１：ケイパビリティの第１要素をｃａｐｆとする。
２：ケイパビリティの第２要素をｌｉｓｔとする。
３：ｃａｐ＝Ｒｎｄ０とする。
４：ｉ＝１とする。
５：ｌｉｓｔの第ｉ番目の要素を取り出し、その第１要素をrightとし、第２要素をＲｎｄとする。
６：ｃａｐが無効リスト保持部に保持されていれば、不正として本処理手順を終了する。そうでなければ、次ステップに進む。
７：ｆ（ｃａｐ，right，Ｒｎｄ）を計算し、ｃａｐの新しい値とする。
８：第ｉ番目の要素が最後の要素の場合はステップ１５に進む。そうでなければ、次ステップに進む
９：ｌｉｓｔの第ｉ＋１番目の要素を取り出し、その第１要素をrightnextとし、第２要素をRndnextとする。
10：rightとrightnextを比較し、権限を弱める方向に正しく変更されているかどうかを調べる。正しければ次ステップに進み、正しくなければ不正として本処理手順を終了する。
11：right = rightnextとする。
12：Ｒｎｄ = Rndnextとする。
13：ｉを１だけ増分する。
14：ステップ８に戻る。
15：ｃａｐｆとｃａｐを比較し、両者が等しければ正しい権限情報とし、等しくなければ不正な権限情報であるとして結果を返す。

【０１８９】但し、一方向性関数ｆとして、下式のような可換性を持つ一方向性関数を用いることもできる。★

【０１９０】

【数１９】

$$f(f(x1, y1, z1), y2, z2) = f(f(x1, y2, z2), y1, z1)$$

【０１９１】可換性のある一方向性関数ｆを用いることにより、変更履歴の順番を無視した下記の《処理手順２》を実行することによっても、《処理手順１》と同様の処理結果が得られる。

【０１９２】

【数２０】

《処理手順２》
１：ケイパビリティの第１要素をｃａｐｆとする。
２：ケイパビリティの第２要素をｌｉｓｔとする。
３：ｃａｐ＝Ｒｎｄ０とする。
４：ｌｉｓｔの任意の要素を取り出し、その第１をrightとし、第２要素をＲｎｄとし、取り出した要素をｌｉｓｔから取り除く。
５：result＝rightとする。
６：ｃａｐが無効リスト保持部に保持されていれば不正として本処理手順を終了する。そうでなければ、次ステップに進む。
７：ｆ（ｃａｐ，right，Ｒｎｄ）を計算し、ｃａｐの新しい値とする。
８：ｌｉｓｔが空リストの場合はステップ１４に進む。そうでなければ次ステップに進む。
９：ｌｉｓｔの任意の要素を取り出し、その第１要素をrightnextとし、第２要素をRndnextとし、取り出した要素をｌｉｓｔから取り除く。
10：rightで表される権限とrightnextで表される権限の最低値をとることによって得られる権限を、resultの新しい値とする。
11：right＝rightnextとする。
12：Ｒｎｄ＝Rndnextとする。
13：ステップ８に戻る。
14：ｃａｐｆとｃａｐを比較し、両者が等しければ正しい権限情報とし、等しくなければ不正な権限情報として結果を返す。

【０１９３】可換性のある一方向性関数ｆを用いることは、ケイパビリティの第２項である変更履歴を表すリストの保持方法として、履歴の順を保持する必要がないことを意味する。例えば、履歴の順番に依らず、権限で許される操作毎にリストを分割して保持したり、権限を特定のビット・フィールドに対応させてリストを保持することが可能となる。

【０１９４】プロキシ・オブジェクト３０１は、《処理手順２》を実行した結果から、メッセージに包含されたケイパビリティの内容は「ｃａｐ１と結び付けられたオブジェクトに対して、世界時刻で１９９８年の４月２４日１０時０分４８秒から１０時５分４８秒の間に、ＧＥＴメソッドを２かい実行することのできる権利」であると判断する。

【０１９５】さらに、プロキシ・オブジェクト３０１は、ケイパビリティ識別子Ｒｎｄ１とＲｎｄ２をキーとして、ケイパビリティ・リスト保持部３３１内を検索する。該当するエントリがリスト中にないので、世界時での現在時刻を取得し、１９９８年４月２４日１０時１分４８秒、すなわち与えられたケイパビリティの有効期限内であることから、ケイパビリティ・リスト保持部３３１中に以下のエントリを保存する。

【０１９６】
【数２１】

ケイパビリティ識別子：Ｒｎｄ１
メ　ソ　ッ　ド：ＧＥＴ
残　り　回　数：４
ケイパビリティ識別子：Ｒｎｄ２
メ　ソ　ッ　ド：ＧＥＴ
残　り　回　数：１

【０１９７】そして、プロキシ・オブジェクト３０１は、該当するＨＴＴＰオブジェクト３９１に対してメッセージＧＥＴを送信するとともに、オブジェクト３９１から受信した応答を要求元のＨＴＴＰクライアントに送信する。

【０１９８】ここで、ＨＴＴＰクライアント５０ＤがＨＴＴＰサーバ３００に対して［数１７］に示したものと同じメッセージを送信した場合の動作について説明する。

【０１９９】プロキシ・オブジェクト３０１は、上述の《処理手順１》または《処理手順２》に従ってメッセージ中の権限情報を検証した後、受信したケイパビリティｃａｐ２に含まれているケイパビリティ識別子Ｒｎｄ１とＲｎｄ２をキーとしてケイパビリティ・リスト保持部３３１を検索し、該当するエントリから以下に示す履歴を抽出する。

【０２００】
【数２２】

ケイパビリティ識別子：Ｒｎｄ１
メ　ソ　ッ　ド：ＧＥＴ
残　り　回　数：４
有　効　期　限：Apr:24:00:00:00:1998:GMT,Apr:25:00:00:00:1998:GMT
ケイパビリティ識別子：Ｒｎｄ２
メ　ソ　ッ　ド：ＧＥＴ
残　り　回　数：１
有　効　期　限：Apr:24:10:00:48:1998:GMT,Apr:25:10:05:48:1998:GMT

【０２０１】そして、プロキシ・オブジェクト３０１は、該当エントリの履歴の内容を以下のように変更してから、対応するＨＴＴＰオブジェクト３９１に対してメッセージＧＥＴを送信する。ここで行われるケイパビリティの変更内容は、残り回数を１だけ減分することである。

【０２０２】
【数２３】

ケイパビリティ識別子：Ｒｎｄ１
メ　ソ　ッ　ド：ＧＥＴ
残　り　回　数：３
有　効　期　限：Apr:24:00:00:00:1998:GMT,Apr:25:00:00:00:1998:GMT
ケイパビリティ識別子：Ｒｎｄ２
メ　ソ　ッ　ド：ＧＥＴ
残　り　回　数：０
有　効　期　限：Apr:24:10:00:48:1998:GMT,Apr:25:10:05:48:1998:GMT

【０２０３】この後、プロキシ・オブジェクト３０１は、世界時で１０時５分４８秒になった時点で、ケイパビリティ・リスト保持部３３１中の識別子Ｒｎｄ２に対応するエントリを削除する（削除しないまでも、エントリに対応するケイパビリティは失効する）。

【０２０４】次に、ＨＴＴＰクライアント５０Ｃが他のＨＴＴＰクライアント５０Ｄに与えたケイパビリティｃａｐ２を無効化する処理について説明する。

※【０２０５】この場合、ＨＴＴＰクライアント５０Ｃは、アクセス識別子ａと、［数１１］に示したケイパビリティｃａｐ１と、ＨＴＴＰクライアント５０Ｄに与えたケイパビリティに含まれるケイパビリティ識別子Ｒｎｄ２を基に、下式［数２４］のようなメッセージを生成して、ＨＴＴＰサーバ３００に送信する。

【０２０６】
【数２４】

ＧＥＴ　/ａ/revocation/ｃａｐ１,ｃａｐ２ HTTP/1.1

【０２０７】このメッセージは、ａというアクセス識別子を持つアクセス権限保持部３２１に対して、ケイパビリティｃａｐ１から派生したケイパビリティｃａｐ２の無効化を要求する旨の内容を含んでいる。

【０２０８】これに対し、プロキシ・オブジェクト３０★１は、以下のような《処理手順３》を実行して、ケイパビリティｃａｐ２がケイパビリティｃａｐ１から派生したものかどうかを検証することができる。

【０２０９】
【数２５】

《処理手順３》
１：ケイパビリティｃａｐ１の変更履歴をhistory1とする。
２：ケイパビリティｃａｐ２の変更履歴をhistory2とする。
３：history1がhistory2の先頭からの連続する部分として含まれるかどうかを調べる。含まれれば次ステップに進み、そうでなければ当該ケイパビリティは派生でないとして、本処理手順を終了する。
４：ケイパビリティｃａｐ２の正当性を《処理手順１》を用いて検証する。正しければ当該ケイパビリティは派生であるとして無効リストにケイパビリティｃａｐ２を追加し、正しくなければ派生ではないとして本処理手順を終了する。

【０２１０】プロキシ・オブジェクト３０１は、無効化要求に含まれる第２のケイパビリティｃａｐ２が第１のケイパビリティｃａｐ１の派生である場合には、要求に含まれるアクセス識別子の無効リスト保持部３４１に当該ケイパビリティｃａｐ２を追加登録する。

【０２１１】なお、無効化されたケイパビリティのうち、そもそも権限の有効期限により無効となるものについては、無効リストから取り除いてもよい。

【０２１２】［追補］以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２１３】

【発明の効果】以上詳記したように、本発明によれば、ネットワーク上に複数のコンピュータ・システムが相互接続された分散型のネットワーク・システムにおいて、ネットワーク上に存在するオブジェクトを安全に保護することができる、優れたオブジェクトのアクセス管理方式を提供することができる。

【０２１４】また、本発明によれば、オブジェクトのアクセス権限を記述したケイパビリティ（Ｃａｐａｂｉｌｉｔｙ）をクライアントに配ることによってオブジェクトへのアクセスを許可するタイプの、優れたアクセス管理方式を提供することができる。

【０２１５】また、本発明によれば、ケイパビリティを保有するクライアントが権限を変更したケイパビリティを自由に生成し、他のクライアントに安全に委譲することができる、優れたオブジェクトのアクセス管理方式を提供することができる。

【０２１６】また、本発明によれば、ケイパビリティを保有するクライアントが権限を変更したケイパビリティ＊を自由に生成し、オブジェクトを管理するサーバは生成されたケイパビリティを安全に検査することができる、優れたオブジェクトのアクセス管理方式を提供することができる。

【０２１７】また、本発明によれば、ケイパビリティを保有するクライアントが権限を変更したケイパビリティを自由に生成し、さらに生成したケイパビリティを確実に無効化することができる、優れたオブジェクトのアクセス管理方式を提供することができる。

【図面の簡単な説明】

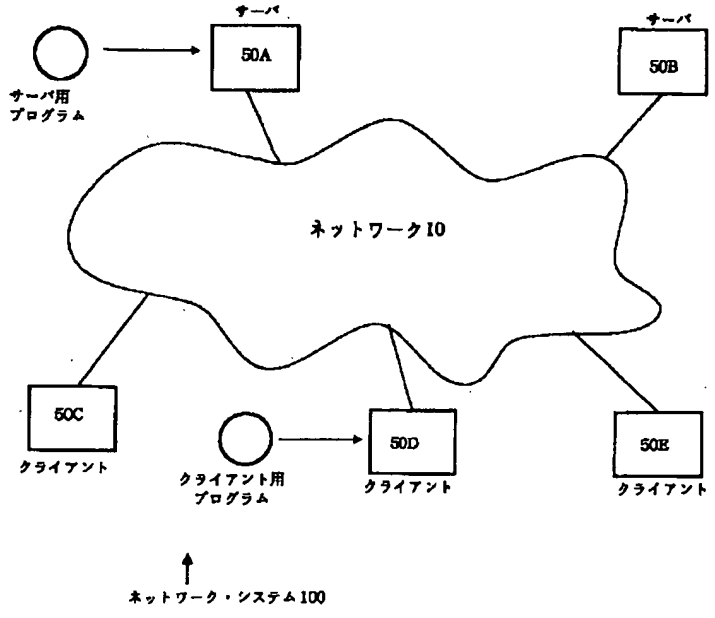
【図１】　本発明の実施に供されるネットワーク・システム１００の構成を模式的に示した図である。

【図２】　オブジェクト・サーバ５０Ａの構成を模式的に示した図である。

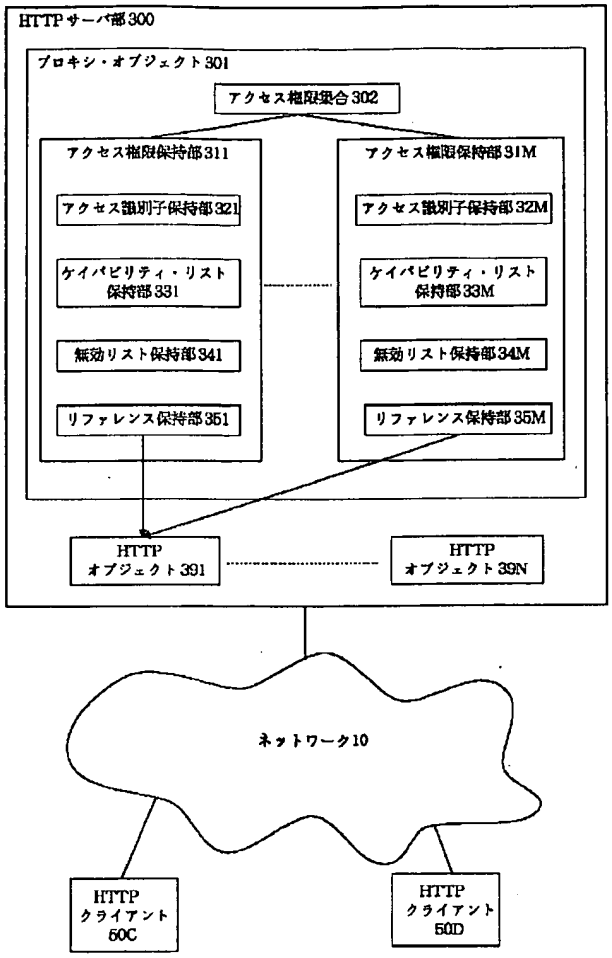
【符号の説明】

１０…ネットワーク
５０…コンピュータ・システム
１００…ネットワーク・システム
３００…ＨＴＴＰサーバ
３０１…プロキシ・オブジェクト
３０２…アクセス権限集合
３１１，３１Ｍ…アクセス権限保持部
３２１，３２Ｍ…アクセス識別子保持部
３３１，３３Ｍ…ケイパビリティ・リスト保持部
３４１，３４Ｍ…無効リスト保持部
３５１，３５Ｍ…リファレンス保持部
３９１，３９Ｍ…ＨＴＴＰオブジェクト

【図１】



【図２】


HTTPサーバ部300
プロキシ・オブジェクト301
アクセス権限集合302
アクセス権限保持部311
アクセス識別子保持部321
ケイパビリティ・リスト保持部331
無効リスト保持部341
リファレンス保持部351
アクセス権限保持部31M
アクセス識別子保持部32M
ケイパビリティ・リスト保持部33M
無効リスト保持部34M
リファレンス保持部35M
HTTPオブジェクト391
HTTPオブジェクト39N
ネットワーク10
HTTPクライアント50C
HTTPクライアント50D